Tópicos de Matemática Elementar: polinômios

Distribuição e vendas
Sociedade Brasileira de Matemática
Estrada Dona Castorina, 110 Sala 109 - Jardim Botânico
22460-320 Rio de Janeiro RJ
Telefones: (21) 2529-5073 / 2529-5095
http://www.sbm.org.br / email:lojavirtual@sbm.org.br

ISBN 978-85-8337-101-4

MUNIZ NETO, Antonio Caminha.
Tópicos de Matemática Elementar:polinômios / Caminha Muniz Neto.
-2.ed. -- Rio de Janeiro: SBM, 2016.
v.6 ; 312 p. (Coleção Professor de Matemática; 29)
ISBN 978-85-8337-101-4

1. Números Complexos. 2. Polinômios. 3. Raízes de Polinômios.
4. Fatoração de Polinômios. I. Título.

Tópicos de Matemática Elementar

Volume 6

Polinômios

Antonio Caminha Muniz Neto

$$\Delta^k f(x_n) = \sum_{i=0}^{k}(-1)^i \binom{k}{i} f(x_{k+n-i}).$$

$$\sum_{p|k}[X^k] = \frac{1}{p}(f(1) + f(\omega) + \cdots + f(\omega^{p-1})).$$

2ª edição
2016
Rio de Janeiro

COLEÇÃO DO PROFESSOR DE MATEMÁTICA

COLEÇÃO DO PROFESSOR DE MATEMÁTICA

- *Logaritmos* - E. L. Lima
- *Análise Combinatória e Probabilidade com as soluções dos exercícios* - A. C. Morgado, J. B. Pitombeira, P. C. P. Carvalho e P. Fernandez
- *Medida e Forma em Geometria (Comprimento, Área, Volume e Semelhança)* - E. L. Lima
- *Meu Professor de Matemática e outras Histórias* - E. L. Lima
- *Coordenadas no Plano com as soluções dos exercícios* - E. L. Lima com a colaboração de P. C. P. Carvalho
- *Trigonometria, Números Complexos* - M. P. do Carmo, A. C. Morgado e E. Wagner, Notas Históricas de J. B. Pitombeira
- *Coordenadas no Espaço* - E. L. Lima
- *Progressões e Matemática Financeira* - A. C. Morgado, E. Wagner e S. C. Zani
- *Construções Geométricas* - E. Wagner com a colaboração de J. P. Q. Carneiro
- *Introdução à Geometria Espacial* - P. C. P. Carvalho
- *Geometria Euclidiana Plana* - J. L. M. Barbosa
- *Isometrias* - E. L. Lima
- *A Matemática do Ensino Médio Vol. 1* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *A Matemática do Ensino Médio Vol. 2* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *A Matemática do Ensino Médio Vol. 3* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *Matemática e Ensino* - E. L. Lima
- *Temas e Problemas* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *Episódios da História Antiga da Matemática* - A. Aaboe
- *Exame de Textos: Análise de livros de Matemática* - E. L. Lima
- *A Matemática do Ensino Medio Vol. 4 - Exercicios e Soluções* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *Construções Geométricas: Exercícios e Soluções* - S. Lima Netto
- *Um Convite à Matemática* - D.C de Morais Filho
- *Tópicos de Matemática Elementar - Volume 1 - Números Reais* - A. Caminha
- Tópicos de *Matemática Elementar - Volume 2 - Geometria Euclidiana Plana* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 3 - Introdução à Análise* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 4 - Combinatória* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 5 - Teoria dos Números* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 6 - Polinômios* - A. Caminha

A meus filhos Gabriel e Isabela,
na esperança de que um dia leiam este livro.

Sumário

Prefácio

Esta coleção evoluiu a partir de sessões de treinamento para olimpíadas de Matemática, por mim ministradas para alunos e professores do Ensino Médio, várias vezes ao longo dos anos de 1992 a 2003 e, mais recentemente, como orientador do Programa de Iniciação Científica para os premiados na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) e do Projeto Amílcar Cabral de cooperação educacional entre Brasil e Cabo Verde.

Idealmente, planejei o texto como uma mistura entre uma iniciação suave e essencialmente autocontida ao fascinante mundo das competições de Matemática, além de uma bibliografia auxiliar aos estudantes e professores do secundário interessados em aprofundar seus conhecimentos matemáticos. Resumidamente, seu propósito primordial é apresentar ao leitor uma abordagem de quase todos os conteúdos geralmente constantes dos currículos do secundário, e que seja ao mesmo tempo concisa, não excessivamente tersa, logicamente estruturada e mais aprofundada que a usual.

Na estruturação dos livros, me ative à máxima do eminente matemático húngaro-americano George Pólya, que dizia não se poder fazer

Matemática sem *sujar as mãos*. Assim sendo, em vários pontos deixei a cargo do leitor a tarefa de verificar aspectos não centrais aos desenvolvimentos principais, quer na forma de detalhes omitidos em demonstrações, quer na de extensões secundárias da teoria. Nestes casos, frequentemente referi o leitor a problemas específicos, os quais se encontram marcados com * e cuja análise e solução considero parte integrante e essencial do texto. Colecionei ainda, em cada seção, outros tantos problemas, cuidadosamente escolhidos na direção de exercitar os resultados principais elencados ao longo da discussão, bem como estendê-los. Uns poucos destes problemas são quase imediatos, ao passo que a maioria, para os quais via de regra oferto sugestões precisas, é razoavelmente difícil; no entanto, insto veementemente o leitor a debruçar-se sobre o maior número possível deles por tempo suficiente para, ainda que não os resolva todos, passar a apreciá-los como corpo de conhecimento adquirido.

O primeiro volume discorre sobre vários aspectos relevantes do conjunto dos números reais e de Álgebra Elementar, no intuito de munir o leitor dos requisitos necessários ao estudo dos tópicos constantes dos volumes subsequentes. Após começar com uma discussão não axiomática das propriedades mais elementares dos números reais, são abordados, em seguida, produtos notáveis, equações e sistemas de equações, sequências elementares, indução matemática e números binomiais; o texto finda com a discussão de várias desigualdades algébricas importantes, notadamente aquela entre as médias aritmética e geométrica, bem como as desigualdades de Cauchy, de Chebyshev e de Abel.

Dedicamos o segundo volume a uma iniciação do leitor à geometria Euclidiana plana, inicialmente de forma não axiomática e enfatizando construções geométricas elementares. Entretanto, à medida em que o texto evolui, o método sintético de Euclides – e, consequentemente, demonstrações – ganha importância, principalmente com a discussão dos conceitos de congruência e semelhança de triângulos; a partir desse ponto, vários belos teoremas clássicos da geometria, usualmente ausentes dos livros-texto do secundário, fazem sua aparição. Numa terceira etapa, o texto apresenta outros métodos elementares usuais no estudo da geometria, quais sejam, o método analítico de R. Descartes, a trigonometria e o uso de vetores; por sua vez, tais métodos são utilizados tanto para reobter resultados anteriores de outra(s) maneira(s) quanto para deduzir novos resultados.

De posse do traquejo algébrico construído no volume inicial e do aparato geométrico do volume dois, discorremos no volume três sobre aspectos elementares de funções e certos excertos de cálculo diferencial e integral e análise matemática, os quais se fazem necessários em certos pontos dos três volumes restantes. Prescindindo, inicialmente, das noções básicas do Cálculo, elaboramos, dentre outros, as noções de gráfico, monotonicidade e extremos de funções, bem como examinamos o problema da determinação de funções definidas implicitamente por relações algébricas. Na continuação, o conceito de função contínua é apresentado, primeiramente de forma intuitiva e, em seguida, axiomática, sendo demonstrados os principais resultados pertinentes. Em especial, utilizamos este conceito para estudar a convexidade de gráficos – culminando com a demonstração da desigualdade de J. Jensen – e o problema da definição rigorosa da área sob o gráfico de uma função contínua e positiva – que, por sua vez, possibilita a apresentação de uma construção adequada das funções logaritmo natural e exponencial. O volume três termina com uma discussão das propriedades mais elementares de derivadas e do teorema fundamental do cálculo, os quais são mais uma vez aplicados ao estudo de desigualdades, em especial da desigualdade entre as médias de potências.

O volume quatro é devotado à análise combinatória. Começamos revisando as técnicas mais elementares de contagem, enfatizando as construções de bijeções e argumentos recursivos como estratégias básicas. Na continuação, apresentamos um apanhado de métodos de contagem um tanto mais sofisticados, como o princípio da inclusão exclusão e os métodos de contagem dupla, do número de classes de

equivalência e mediante o emprego de métricas em conjuntos finitos. A cena é então ocupada por funções geradoras, onde a teoria elementar de séries de potências nos permite discutir de outra maneira problemas antigos e introduzir problemas novos, antes inacessíveis. Terminada nossa excursão pelo mundo da contagem, enveredamos pelo estudo do problema da existência de uma configuração especial no universo das configurações possíveis, utilizando para tanto o princípio das gavetas de G. L. Dirichlet – vulgo "princípio das casas dos pombos" –, um célebre teorema de R. Dilworth e a procura e análise de invariantes associados a problemas algorítmicos. A última estrutura combinatória que discutimos é a de um grafo, quando apresentamos os conceitos básicos usuais da teoria com vistas à discussão de três teoremas clássicos importantes: a caracterização da existência de caminhos Eulerianos, o teorema de A. Cayley sobre o número de árvores rotuladas e o teorema extremal de P. Turán sobre a existência de subgrafos completos em um grafo.

Passamos em seguida, no quinto volume, à discussão dos conceitos e resultados mais elementares de teoria dos números, ressaltando-se inicialmente a teoria básica do máximo divisor comum e o teorema fundamental da aritmética. Discutimos também o método da descida de P. de Fermat como ferramenta para provar a inexistência de soluções inteiras para certas equações diofantinas, e resolvemos também a famosa equação de J. Pell. Em seguida, preparamos o terreno para a discussão do famoso teorema de Euler sobre congruências, construindo a igualmente famosa função de Euler com o auxílio da teoria mais geral de funções aritméticas multiplicativas. A partir daí, o livro apresenta formalmente o conceito de congruência de números em relação a um certo módulo, discutindo extensivamente os resultados usualmente constantes dos cursos introdutórios sobre o assunto, incluindo raízes primitivas, resíduos quadráticos e o teorema de Fermat de caracterização dos inteiros que podem ser escritos como soma de dois quadrados. O grande diferencial aqui, do nosso ponto de vista, é o calibre dos

exemplos discutidos e dos problemas propostos ao longo do texto, boa parte dos quais oriundos de variadas competições ao redor do mundo.

Finalmente, números complexos e polinômios são os objetos de estudo do sexto e último volume da coleção. Para além da teoria correspondente usualmente estudada no secundário – como a noção de grau, o algoritmo da divisão e o conceito de raízes de polinômios –, vários são os tópicos não padrão abordados aqui. Dentre outros, destacamos inicialmente a utilização de números complexos e polinômios como ferramentas de contagem e a apresentação quase completa de uma das mais simples demonstrações do teorema fundamental da álgebra. A seguir, estudamos o famoso teorema de I. Newton sobre polinômios simétricos e as igualmente famosas desigualdades de Newton, as quais estendem a desigualdade entre as médias aritmética e geométrica. O próximo tema concerne os aspectos básicos da teoria de interpolação de polinômios, quando dispensamos especial atenção aos polinômios interpoladores de J. L. Lagrange. Estes, por sua vez, são utilizados para resolver sistemas lineares de Vandermonde sem o recurso à álgebra linear, os quais, a seu turno, possibilitam o estudo de uma classe particular de sequências recorrentes lineares. O livro termina com o estudo das propriedades de fatoração de polinômios com coeficientes inteiros, racionais ou pertencentes ao conjunto das classes de congruência relativas a algum módulo primo, seguido do estudo do conceito de número algébrico. Há, aqui, dois pontos culminantes: por um lado, uma prova mais simples do fechamento do conjunto dos números algébricos em relação às operações aritméticas básicas; por outro, o emprego de polinômios ciclotômicos para provar um caso particular do teorema de Dirichlet sobre primos em progressões aritméticas.

Várias pessoas contribuíram ao longo dos anos, direta ou indiretamente, para que um punhado de anotações em cadernos pudesse transformar-se nesta coleção de livros. Os ex-professores do Departamento de Matemática da Universidade Federal do Ceará, Marcondes

Cavalcante França, João Marques Pereira, Guilherme Lincoln Aguiar Ellery e Raimundo Thompson Gonçalves, ao criarem a Olimpíada Cearense de Matemática na década de 1980, motivaram centenas de jovens cearenses, dentre os quais eu me encontrava, a estudarem mais Matemática. Meu ex-professor do Colégio Militar de Fortaleza, Antônio Valdenísio Bezerra, ao convidar-me, inicialmente para assistir a suas aulas de treinamento para a Olimpíada Cearense de Matemática e posteriormente para dar aulas consigo, iniciou-me no maravilhoso mundo das competições de Matemática e influenciou definitivamente minha escolha profissional. Os comentários de muitos de vários de ex-alunos contribuíram muito para o formato final de boa parte do material aqui colecionado; nesse sentido, agradeço especialmente a João Luiz de Alencar Araripe Falcão, Roney Rodger Sales de Castro, Marcelo Mendes de Oliveira, Marcondes Cavalcante França Jr., Marcelo Cruz de Souza, Eduardo Cabral Balreira, Breno de Alencar Araripe Falcão, Fabrício Siqueira Benevides, Rui Facundo Vigelis, Daniel Pinheiro Sobreira, Antônia Taline de Souza Mendonça, Carlos Augusto David Ribeiro, Samuel Barbosa Feitosa, Davi Máximo Alexandrino Nogueira e Yuri Gomes Lima. Vários de meus colegas professores teceram comentários pertinentes, os quais foram incorporados ao texto de uma ou outra maneira; agradeço, em especial, a Fláudio José Gonçalves, Francisco José da Silva Jr., Onofre Campos da Silva Farias, Emanuel Augusto de Souza Carneiro, Marcelo Mendes de Oliveira, Samuel Barbosa Feitosa e Francisco Bruno de Lima Holanda. Os professores João Lucas Barbosa e Hélio Barros deram-me a conclusão de parte destas notas como alvo a perseguir ao me convidarem a participar do Projeto Amílcar Cabral de treinamento dos professores de Matemática da República do Cabo Verde. Meus colegas do Departamento de Matemática da Universidade Federal do Ceará, Abdênago Alves de Barros, José Othon Dantas Lopes, José Robério Rogério e Fernanda Esther Camillo Camargo, bem como meu orientando de iniciação científica Itamar Sales de Oliveira Filho, leram partes do texto final e ofereceram várias sugestões. Os pareceristas indicados pela SBM opinaram decisivamente para que os livros certamente resultassem melhores que a versão inicial por mim submetida. O presidente da SBM, professor Hilário Alencar da Silva, o antigo editor-chefe da SBM, professor Roberto Imbuzeiro de Oliveira, bem como o novo editor-chefe, professor Abramo Hefez, foram sempre extremamente solícitos e atenciosos comigo ao longo de todo o processo de edição. Por fim, quaisquer erros ou incongruências que ainda se façam presentes, ou omissões na lista acima, são de minha inteira responsabilidade.

Por fim e principalmente, gostaria de agradecer a meus pais, Antonio Caminha Muniz Filho e Rosemary Carvalho Caminha Muniz, e à minha esposa Mônica Valesca Mota Caminha Muniz. Meus pais me fizeram compreender a importância do conhecimento desde a mais tenra idade, sem nunca terem medido esforços para que eu e meus irmãos desfrutássemos o melhor ensino disponível; minha esposa brindou-me com a harmonia e o incentivo necessários à manutenção de meu ânimo e humor, em longos meses de trabalho solitário nas madrugadas. Esta coleção de livros também é dedicada a eles.

FORTALEZA, JANEIRO de 2012

Antonio Caminha M. Neto

Prefácio à segunda edição

A segunda edição contempla uma extensa revisão do texto e dos problemas propostos, tendo sido corrigidas várias imprecisões de língua portuguesa e de Matemática. A discussão sobre recorrências lineares foi ampliada, no que resultou o capítulo 9, inteiramente dedicado a elas. Nele, a solução de recorrências lineares de coeficientes constantes gerais é apresentada, sendo demonstrada com o auxílio de funções geradoras complexas. Apesar dessa ser uma abordagem natural para este problema, salta aos olhos não haver tratamento adequado desse tema disponível em língua portuguesa. Há, ainda, uma nova seção no capítulo 8, versando sobre números transcendentes. Nela, a prova original de J. Liouville para a existência de números transcendentes é demonstrada. Adicionei também alguns exemplos e problemas novos, no intuito de melhor exercitar certos pontos da teoria, os quais não se encontravam adequadamente contemplados pelos problemas propostos à primeira edição. As sugestões e soluções aos problemas propostos também foram revistas e reorganizadas, tendo sido colecionadas em um capítulo separado, o capítulo 10. Adicionalmente, são apresentadas sugestões ou soluções a praticamente todos os problemas do livro.

Gostaria de aproveitar o ensejo para agradecer à comunidade matemática brasileira em geral, e a todos os leitores que me enviaram sugestões ou correções em particular, o excelente acolhimento desfrutado pela primeira edição desta obra.

FORTALEZA, JULHO de 2016

Antonio Caminha M. Neto

CAPÍTULO 1

Números Complexos

É um fato óbvio que o conjunto dos números reais resulta pequeno demais para uma descrição completa das raízes de funções polinomiais reais; por exemplo, a função $x \mapsto x^2+1$, $x \in \mathbb{R}$, não as possui. Historicamente, afirmações simples como essa motivaram o desenvolvimento dos números complexos, coroado pela demonstração, por Gauss, do famoso *teorema fundamental da álgebra*.

Neste capítulo, concentramo-nos na construção do conjunto dos números complexos e na discussão de suas propriedades mais elementares, postergando ao capítulo 3 a apresentação de uma demonstração quase completa do teorema de Gauss acima referido.

1.1 Definição e propriedades elementares

Conforme visto no capítulo 1 de [10], em geral pensamos no conjunto $\mathbb{R}$ dos números reais como uma *reta numerada*: temos uma

reta qualquer (entidade geométrica) disposta horizontalmente, na qual marcamos um ponto (correspondente ao zero). A partir daí, escolhemos um comprimento padrão (que corresponderá à unidade) e duas regras distintas para operar dois pontos da reta (denominadas adição e multiplicação de números reais), de modo a obter um terceiro ponto como resultado. Então, chamamos os pontos da reta de números e verificamos que as operações definidas gozam de várias propriedades úteis: comutatividade, associatividade etc.

A discussão acima suscita a seguinte pergunta natural: haveria alguma forma de introduzir *operações com propriedades úteis* para os pontos de um plano? Mais precisamente, se considerarmos a reta real como o eixo horizontal de um plano cartesiano, haveria um modo de definirmos operações com os pontos desse plano, generalizando as operações com os pontos da reta real? A resposta é *sim* e o conjunto resultante, que passamos a descrever, é o conjunto dos *números complexos*.

Considere o plano cartesiano, visto como o conjunto $\mathbb{R} \times \mathbb{R}$ dos pares ordenados (a, b) de números reais. Defina em tal plano as operações $\oplus$ e $\odot$ por

$$(a,b)\oplus(c,d) = (a+c, b+d), \quad (a,b)\odot(c,d) = (ac-bd, ad+bc), \quad (1.1)$$

onde $+$ e $\cdot$ denotam a adição e a multiplicação usuais de números reais.

Podemos verificar sem dificuldade que $\oplus$ e $\odot$ são operações *associativas* e *comutativas* e que $\odot$ é distributiva em relação a $\oplus$, i.e., que, para todos $a, b, c, d, e, f \in \mathbb{R}$, valem as seguintes propriedades:

i. **Associatividade** de $\oplus$ e $\otimes$: $(a, b) \oplus ((c, d) \oplus (e, f)) = ((a, b) \oplus (c, d)) \oplus (e, f)$ e $(a, b) \odot ((c, d) \odot (e, f)) = ((a, b) \odot (c, d)) \odot (e, f)$.

ii. **Comutatividade** de $\oplus$ e $\otimes$: $(a, b) \oplus (c, d) = (c, d) \oplus (a, b)$ e $(a, b) \odot (c, d) = (c, d) \odot (a, b)$.

iii. **Distributividade** de $\otimes$ em relação a $\oplus$: $(a, b)\odot((c, d)\oplus(e, f)) = ((a, b) \odot (c, d)) \oplus ((a, b) \odot (e, f))$

Também é imediato verificar que $(0, 0)$ e $(1, 0)$ são, respectivamente, os **elementos neutros** de $\oplus$ e $\odot$, i.e., que

$$(a, b) \oplus (0, 0) = (a, b) \quad \text{e} \quad (a, b) \odot (1, 0) = (a, b),$$

para todos $a, b \in \mathbb{R}$. Podemos ainda checar (faça isto!) que vale a seguinte **lei de cancelamento** para $\odot$:

$$(a, b) \odot (c, d) = (0, 0) \Rightarrow (a, b) = (0, 0) \quad \text{ou} \quad (c, d) = (0, 0).$$

Considere, agora, nossa reta real como sendo o eixo das abscissas, o que equivale a identificar cada real x com o ponto $(x, 0)$. Temos, então, que ver se essa identificação é boa, no sentido de os resultados das operações $\oplus$ e $\odot$ coincidirem com os correspondentes das operações usuais de adição e multiplicação de números reais. Isto se resume a verificarmos se

$$(x, 0) \oplus (y, 0) = (x + y, 0) \quad \text{e} \quad (x, 0) \odot (y, 0) = (xy, 0), \qquad (1.2)$$

o que é imediato fazer.

Em palavras, as expressões acima dizem que, ao identificarmos os números reais com os pontos do eixo das abscissas e executarmos as operações $\oplus$ e $\odot$ acima definidas, obtemos os mesmos resultados que obteríamos se, primeiro, executássemos as operações usuais de adição e multiplicação com os números reais e, só então, identificássemos os resultados assim obtidos com os pontos do eixo das abscissas.

Portanto, podemos considerar $\mathbb{R}$ com suas operações usuais de adição e multiplicação como um subconjunto de $\mathbb{R} \times \mathbb{R}$ com as operações $\oplus$ e $\odot$, definidas como em (1.1), e também chamar os pontos do plano de números, mais precisamente de **números complexos**. Denotamos o conjunto dos números complexos por $\mathbb{C}$.

No que segue, vamos obter um modo mais cômodo de representar os números complexos e suas operações. Para tanto, denotaremos doravante por i o elemento $(0, 1)$ do conjunto dos complexos e

o denominaremos a **unidade imaginária**[1]. Denotando por $\approx$ nossa identificação dos pontos do eixo das abscissas com os números reais e levando em conta a definição de $\odot$, somos forçados a concluir que

$$i^2 = (0,1) \odot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0) \approx -1. \quad (1.3)$$

Veja, ainda, que

$$(a,b) = (a,0) \oplus (0,b) = (a,0) \oplus ((b,0) \odot (0,1)) \approx a + bi. \quad (1.4)$$

Doravante, denotaremos as operações $\oplus$ e $\odot$ simplesmente por $+$ e $\cdot$, e escreveremos $a + bi$ para denotar o número complexo (a, b), não mais utilizando identificações. Segue, a partir de (1.4), que

$$a + bi = 0 \Leftrightarrow (a,b) = (0,0) \Leftrightarrow a = b = 0.$$

Por outro lado, veja que, de acordo com a discussão acima, no conjunto $\mathbb{C}$ dos números complexos a equação

$$x^2 + 1 = 0$$

tem o número i por raiz. Como veremos ao longo deste capítulo, esse fato é o cerne da importância dos números complexos.

Uma boa justificativa para podermos escrever $(a, b) \in \mathbb{C}$ como $a+bi$ é que podemos operar com os complexos escritos na forma $a+bi$ como fazemos com números reais, lembrando que $i^2 = -1$: os cálculos feitos desse modo levam aos mesmos resultados que os cálculos feitos usando diretamente as definições das operações $+$ e $\cdot$ de $\mathbb{C}$. Senão, vejamos:

[1]As nomenclaturas *imaginária* e *complexos* têm origens históricas. Mais precisamente, quando os primeiros matemáticos começaram a utilizar números complexos, ainda sem uma definição precisa do que tais números seriam, chamaram-nos *complexos* ou *imaginários* exatamente pela estranheza que causara cogitar-se a existência de "números" cujos quadrados pudessem ser negativos.

- Cálculo de $(a,b) + (c,d)$: por definição, temos $(a,b) + (c,d) = (a+c, b+d)$. Por outro lado, operando como usualmente fazemos com números reais, obtemos

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

  Mas, como estamos escrevendo $(a+c, b+d) = (a+c) + (b+d)i$, os dois resultados coincidem.

- Cálculo de $(a,b) \cdot (c,d)$: por definição, temos $(a,b) \cdot (c,d) = (ac - bd, ad + bc)$. Operando novamente como com números reais, temos

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i,$$

  uma vez que $i^2 = -1$. Mas, como estamos escrevendo $(ac - bd, ad + bc) = (ac - bd) + (ad + bc)i$, os resultados novamente coincidem.

Levando em consideração as identificações feitas acima, podemos escrever $\mathbb{R} \subset \mathbb{C}$. Ademais, por analogia com as operações de adição e multiplicação dos reais, também denominaremos as operações $+$ e $\cdot$ sobre complexos de **adição** e **multiplicação**, respectivamente.

Prosseguindo nosso estudo, vamos introduzir em $\mathbb{C}$ outras duas operações, semelhantes à subtração e à divisão de números reais.

Dados $z, w \in \mathbb{C}$, *subtrair* w de z significa obter um complexo $z - w$ (a *diferença* entre z e w) tal que $z = (z - w) + w$. Sendo $z = a + bi$ e $w = c + di$ e operando como com números reais, vê-se facilmente que

$$z - w = (a + bi) - (c + di) = (a - c) + (b - d)i.$$

Assim, sendo $z = a + bi$ e $w = c + di$, o número complexo $z - w$, definido por

$$z - w = (a - c) + (b - d)i, \quad (1.5)$$

é denominado a **diferença** entre z e w.

Para $z, w \in \mathbb{C}$, com $w \neq 0$, *dividir* z por w significa obter um número complexo z/w (o *quociente* entre z e w), tal que $z = (z/w) \cdot w$. Sendo $z = a + bi$ e $w = c + di$ e operando como quando fazemos racionalizações com números reais, obtemos imediatamente

$$\begin{aligned} \frac{z}{w} = \frac{a+bi}{c+di} &= \frac{(a+bi)(c-di)}{(c+di)(c-di)} \\ &= \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} \\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i. \end{aligned}$$

Sendo $z = a + bi$ e $w = c + di$, com $w \neq 0$, o número complexo z/w, definido por

$$\frac{z}{w} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i, \tag{1.6}$$

é o **quociente** entre z e w.

Examinando o caso particular da divisão de 1 por um número complexo não nulo, concluímos que todo complexo $z \neq 0$ possui inverso em relação à multiplicação. Sendo $z = a + ib \neq 0$, segue de (1.6) que tal inverso, o qual denotaremos z^{-1} ou $1/z$, é dado por

$$z^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Lembre-se de que não precisamos nos preocupar em decorar as fórmulas acima. É só operar como quando operamos com números reais.

A fim de simplificar muitos de nossos cálculos posteriores, introduzimos, agora, a seguinte notação: para $z = a + bi \in \mathbb{C}$, denotamos por $\overline{z}$ o complexo $\overline{z} = a - bi$ e o denominamos o **conjugado** de z. Em particular, temos $\overline{\overline{z}} = z$.

Observe ainda que, ao multiplicar z por $\overline{z}$, obtemos como resultado o número real $a^2 + b^2$:

$$z \cdot \overline{z} = (a+bi)(a-bi) = a^2 - (bi)^2 = a^2 + b^2.$$

Denotamos $|z| = \sqrt{a^2+b^2}$ e denominamos $|z|$ o **módulo** de z. Quando $z \in \mathbb{R}$, é imediato que a noção de módulo de um número complexo, definida como acima, coincide com a noção usual de módulo de um número real. Note também que, em resumo,

$$z = a + bi \Rightarrow |z|^2 = z\overline{z} = a^2 + b^2. \tag{1.7}$$

Olhando os pontos do plano cartesiano como o conjunto $\mathbb{C}$ dos complexos, obtemos uma representação geométrica de $\mathbb{C}$ conhecida como o **plano complexo**[2].

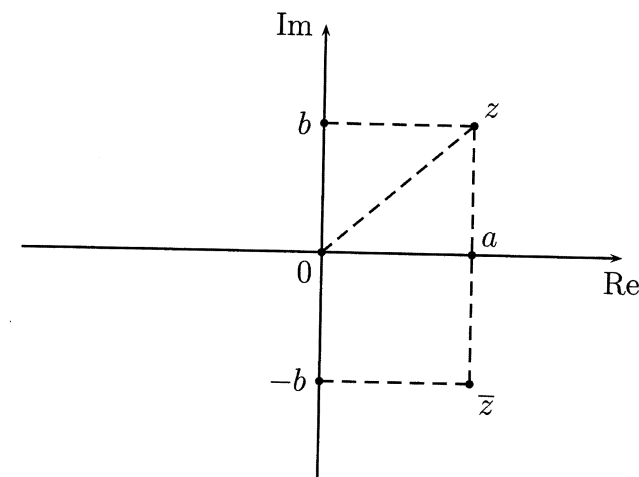



Figura 1.1: conjugação de números complexos.

Os eixos horizontal e vertical do plano complexo são denominados, respectivamente, eixos **real** e **imaginário**. O eixo real é formado pelos números complexos reais (i.e., os pares ordenados $(x, 0) \approx x$), ao passo que o eixo imaginário é formado pelos números complexos da forma

[2]também chamado *plano de Argand-Gauss*, em homenagem aos matemáticos Jean-Robert Argand e Johann Carl Friedrich Gauss.

yi, onde $y \in \mathbb{R}$ (i.e., os pares ordenados $(0, y) = (y, 0) \cdot (0, 1) \approx yi$); tais números complexos são denominados **imaginários puros**.

Ainda em relação ao plano complexo, sendo $z = a + bi = (a, b)$, segue de $\overline{z} = a - bi$ que z e $\overline{z}$ são simétricos em relação ao eixo real (veja a figura 1.1). Por outro lado, os números reais a e b são respectivamente denominados a **parte real** e a **parte imaginária** de z, e denotados

$$a = \text{Re}(z), \quad b = \text{Im}(z).$$

É, agora, claro que

$$\text{Re}(z) = \frac{z + \overline{z}}{2} \text{ e } \text{Im}(z) = \frac{z - \overline{z}}{2i}. \tag{1.8}$$

O resultado a seguir traz mais algumas propriedades úteis dos números complexos. Para o enunciado do mesmo, observamos que a associatividade da multiplicação de números complexos garante a boa definição de z^n, para $z \in \mathbb{C}$ e $n \in \mathbb{N}$, como $z^1 = z$ e

$$z^n = \underbrace{z \cdot \ldots \cdot z}_{n \text{ vezes}},$$

para $n > 1$. Tal definição pode ser facilmente estendida a expoentes inteiros n, pondo, para $z \in \mathbb{C} \setminus \{0\}$, $z^0 = 1$ e

$$z^n = (z^{-n})^{-1} = \frac{1}{z^{-n}},$$

para $n < 0$ inteiro. Então, uma fácil indução permite mostrar que as regras usuais de potenciação continuam válidas, a saber, que

$$(z^m)^n = z^{mn} \text{ e } (zw)^n = z^n w^n, \tag{1.9}$$

para todos $z, w \in \mathbb{C} \setminus \{0\}$ e $m, n \in \mathbb{Z}$.

Podemos, finalmente, enunciar e provar o resultado desejado.

Lema 1.1. *Se z e w são complexos não nulos quaisquer, então:*

(a) $z \in \mathbb{R} \Leftrightarrow \text{Re}(z) = 0 \Leftrightarrow z = \overline{z}$.

(b) $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z} \cdot \overline{w}$ *e* $\overline{z/w} = \overline{z}/\overline{w}$.

(c) $\overline{z^n} = (\overline{z})^n$, *para todo* $n \in \mathbb{Z}$.

(d) $|z| = 1 \Leftrightarrow \overline{z} = 1/z$.

Prova.
(a) Seja $z = a + bi$. Temos

$$z \in \mathbb{R} \Leftrightarrow b = 0 \Leftrightarrow a + bi = a - bi \Leftrightarrow z = \overline{z}.$$

(b) Sendo $z = a + bi$ e $w = c + di$, temos

$$\begin{aligned} \overline{z} + \overline{w} &= (a - bi) + (c - di) \\ &= (a + c) - (b + d)i \\ &= \overline{z + w} \end{aligned}$$

e

$$\begin{aligned} \overline{zw} &= \overline{(ac - bd) + (ad + bc)i} \\ &= (ac - bd) - (ad + bc)i \\ &= (a - bi)(c - di) \; = \; \overline{z} \cdot \overline{w}. \end{aligned}$$

A partir daí, vem

$$\overline{z/w} \cdot \overline{w} = \overline{z/w \cdot w} = \overline{z},$$

de maneira que

$$\overline{z/w} = \overline{z}/\overline{w}.$$

(c) Para $n = 0$ o resultado é imediato e, para $n \in \mathbb{N}$, segue facilmente de (b), por indução. Para $n < 0$ inteiro, observe inicialmente que, pelo item (b), temos

$$1 = \overline{1} = \overline{zz^{-1}} = \overline{z} \cdot \overline{z^{-1}},$$

de sorte que $\overline{z^{-1}} = (\overline{z})^{-1}$; portanto, pondo $u = z^{-1}$, a primeira parte acima, juntamente com (1.9), fornece

$$\overline{z^n} = \overline{u^{-n}} = (\overline{u})^{-n} = ((\overline{z})^{-1})^{-n} = (\overline{z})^{(-1)(-n)} = (\overline{z})^n.$$

(d) Uma vez que (cf. (1.7)) $z \cdot \overline{z} = |z|^2$, concluímos que

$$|z| = 1 \Leftrightarrow z \cdot \overline{z} = 1 \Leftrightarrow \overline{z} = 1/z.$$

□

Exemplo 1.2 (Espanha). *Se z e w são números complexos de módulo 1 e tais que $zw \neq -1$, mostre que $\frac{z+w}{1+zw}$ é um número real.*

Prova. Se $a = \frac{z+w}{1+zw}$, basta mostrarmos que $\overline{a} = a$. Para tanto, note que, pelo lema anterior, temos

$$\begin{aligned}\overline{a} &= \frac{\overline{z+w}}{\overline{1+zw}} = \frac{\overline{z}+\overline{w}}{1+\overline{z}\cdot\overline{w}} \\ &= \frac{z^{-1}+w^{-1}}{1+z^{-1}w^{-1}} = \frac{w+z}{zw+1} = a.\end{aligned}$$

□

Nosso próximo resultado dá uma interpretação geométrica bastante útil do módulo da diferença de dois números complexos.

Proposição 1.3. *Dados $z, w \in \mathbb{C}$, o número real $|z-w|$ é igual à distância Euclidiana de z a w no plano cartesiano subjacente ao plano complexo em questão.*

Prova. Se $z = a + bi$, $w = c + di$, então

$$|z-w| = |(a-c) + (b-d)i| = \sqrt{(a-c)^2 + (b-d)^2}.$$

Por outro lado (conforme a figura 1.2), a proposição 6.5 de [11] garante que a distância de z a w também é dada por $\sqrt{(a-c)^2 + (b-d)^2}$. □

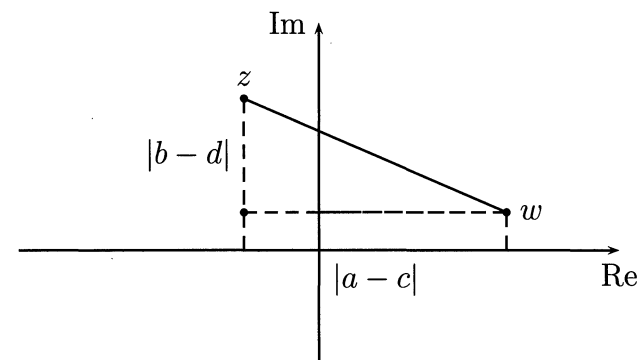



Figura 1.2: módulo da diferença entre dois complexos.

A desigualdade (1.10), a seguir, é conhecida como a **desigualdade triangular** para números complexos.

Corolário 1.4. *Se u, v e z são números complexos quaisquer, então*

$$|u-v| \leq |u-z| + |z-v|. \tag{1.10}$$

Prova. De acordo com a proposição 1.3, o corolário diz apenas que qualquer lado de um triângulo (possivelmente degenerado) é menor ou igual que a soma dos outros dois lados, o que já sabemos ser verdadeiro (conforme ensina a proposição 2.26 de [11]). □

Problemas – Seção 1.1

1. Em relação às operações de adição e multiplicação de números complexos, verifique, a partir da definição, a associatividade e comutatividade, bem como a distributividade da multiplicação com respeito à adição. Verifique, ainda, que $(0,0)$ e $(1,0)$ são,

respectivamente, seus elementos neutros e que vale a lei do cancelamento para a multiplicação.

2. * Para $z, w \in \mathbb{C}$, prove que:

   (a) $|zw| = |z| \cdot |w|$.

   (b) $|z + w|^2 = |z|^2 + 2\text{Re}(\overline{z}w) + |w|^2$.

3. * Use o item (b) do problema anterior para provar, para todos $z, w \in \mathbb{C}$, a validade da desigualdade $|z + w| \leq |z| + |w|$, a qual também é conhecida como a **desigualdade triangular** para números complexos. Em seguida, use essa desigualdade para:

   (a) Deduzir a validade de (1.10).

   (b) Provar que $||z| - |w|| \leq |z - w|$, para todos $z, w \in \mathbb{C}$.

4. Para $z \in \mathbb{C}$, prove que $|z| = 1$ se, e só se, existe $x \in \mathbb{R}$ tal que $z = \frac{1-ix}{1+ix}$.

5. (OCM.) Sejam a e z números complexos tais que $|a| < 1$ e $\overline{a}z \neq 1$. Se
$$\left|\frac{z - a}{1 - \overline{a}\,z}\right| < 1,$$
prove que $|z| < 1$.

Para o próximo problema, definimos uma sequência de números complexos como uma função $f : \mathbb{N} \to \mathbb{C}$. Parafraseando nossa discussão sobre sequências de números reais, levada a cabo em [12], dada uma sequência $f : \mathbb{N} \to \mathbb{C}$, escrevemos $z_n = f(n)$ e nos referimos à sequência f simplesmente por $(z_n)_{n\geq 1}$.

6. (Holanda.) A sequência $(z_k)_{k\geq 1}$ de números complexos é definida, para $k \in \mathbb{N}$, por
$$z_k = \prod_{j=1}^{k}\left(1 + \frac{i}{\sqrt{j}}\right),$$
onde i é a unidade imaginária. Encontre todos os $n \in \mathbb{N}$ tais que
$$\sum_{k=1}^{n} |z_{k+1} - z_k| = 1000.$$

7. Dados $z, w \in \mathbb{C}$, sejam $\mathbf{u}$ e $\mathbf{v}$ os vetores de origem 0 e extremidades respectivamente z e w. Prove que os números complexos $z + w$ e $z - w$ são, respectivamente, as extremidades dos vetores $\mathbf{u} + \mathbf{v}$ e $\mathbf{u} - \mathbf{v}$, com origem em 0.

Para o próximo problema, recorde que (de acordo com a seção 4.2 de [13]) uma **relação de ordem** (**parcial**) em X é uma relação $\preceq$ em X que é *reflexiva*, *transitiva* e *antissimétrica*; ademais, se tivermos $x \preceq y$ ou $y \preceq x$ para todos $x, y \in X$, a relação de ordem $\preceq$ é dita **total**. Para exemplificar, veja que a relação $\preceq$, definida em $\mathbb{R}$ por
$$x \preceq y \Leftrightarrow x \leq y,$$
é uma relação de ordem total; por outro lado, a relação $\preceq$ em $\mathbb{N}$, definida (veja o capítulo 1 de [14]) por
$$x \preceq y \Leftrightarrow x \mid y,$$
é uma relação de ordem parcial que não é total.

8. Prove que o conjunto dos números complexos não pode ser totalmente ordenado. Mais precisamente, prove que não existe,

sobre $\mathbb{C}$, uma relação de ordem total $\preceq$, a qual estende a relação de ordem usual em $\mathbb{R}$ e satisfaz as condições

$$0 \preceq z, w \Rightarrow 0 \preceq z + w, zw.$$

O próximo problema generaliza a construção do conjunto dos números complexos, apresentando a construção do conjunto $\mathbb{H}$ dos **quatérnios** (ou, ainda, **números quaterniônicos**) de Hamilton[3].

9. Em $\mathbb{H} = \{(a, b, c, d);\ a, b, c, d, \in \mathbb{R}\}$, defina operações $\oplus$ e $\odot$, denominadas respectivamente adição e multiplicação, pondo, para $\alpha = (a, b, c, d)$ e $\beta = (w, x, y, z)$ em $\mathbb{H}$,

$$\alpha \oplus \beta = (a + w, b + x, c + y, d + z)$$

e

$$\alpha \odot \beta = (aw - bx - cy - dz, ax + bw + cz - dy, ay - bz + cw + dx, az + by - cx + dw),$$

onde $+$ e $\cdot$ denotam as operações usuais de adição e multiplicação de números reais. Faça os seguintes itens:

(a) Mostre que a função $\iota : \mathbb{R} \to \mathbb{H}$, tal que $\iota(x) = (x, 0, 0, 0)$ preserva operações, no sentido de que

$$\iota(x) \oplus \iota(y) = \iota(x + y) \quad \text{e} \quad \iota(x) \odot \iota(y) = \iota(x + y),$$

para todos $x, y \in \mathbb{R}$.

[3] Após o matemático inglês do século XIX William R. Hamilton. O conjunto dos quatérnios tem muitas aplicações importantes em Matemática e em Física, mas estas fogem ao escopo destas notas.

(b) Mostre que as funções $\iota_1, \iota_2, \iota_3 : \mathbb{C} \to \mathbb{H}$, tais que $\iota_1(x+yi) = (x, y, 0, 0)$, $\iota_2(x + yi) = (x, 0, y, 0)$ e $\iota_3(x + yi) = (x, 0, 0, y)$, preservam operações, no sentido de que

$$\iota_j(z) \oplus \iota_j(w) = \iota_j(z + w) \quad \text{e} \quad \iota_j(z) \odot \iota_j(w) = \iota_j(z + w),$$

para todos $z, w \in \mathbb{C}$ e $1 \leq j \leq 3$.

(c) De posse dos itens (a) e (b), escrevamos, doravante, simplesmente $+$ e $\cdot$ para denotar $\oplus$ e $\odot$, respectivamente, x para denotar $(x, 0, 0, 0)$ e $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ e $k = (0, 0, 0, 1)$. Mostre que

$$\begin{aligned} &i^2 = j^2 = k^2 = -1 \\ &ij = -ji = k, jk = -kj = i, ki = -ik = j \end{aligned} \tag{1.11}$$

e

$$(a, b, c, d) = a + bi + cj + dk.$$

(d) Mostre que os resultados de $(a + bi + cj + dk) + (w + xi + yj + zk)$ e $(a + bi + cj + dk) \cdot (w + xi + yj + zk)$ são os mesmos que obteríamos utilizando as propriedades usuais da adição e da multiplicação de números reais, juntamente com as relações (1.11). A partir daí, conclua que:

i. A operação $+$ é comutativa, associativa e tem 0 como elemento neutro.

ii. A operação é associativa, distributiva em relação a $+$, tem 1 como elemento neutro mas não é comutativa.

(e) Para $\alpha = a + bi + cj + dk \in \mathbb{H}$, sejam $\overline{\alpha} = a - bi - cj - dj$ o **conjugado** de α. Mostre que, para $\alpha, \beta \in \mathbb{H}$, temos $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.

(f) Para $\alpha = a + bi + cj + dk \in \mathbb{H}$, seja $|\alpha| = \sqrt{a^2 + b^2 + c^2 + d^2}$ a **norma** de α. Mostre que $\alpha\overline{\alpha} = |\alpha|^2$ e $|\alpha\beta| = |\alpha||\beta|$, para todos $\alpha, \beta \in \mathbb{H}$.

(g) Use o resultado do item anterior para deduzir a identidade (7.9) de [14].

(h) Conclua que, para todo $\alpha \in \mathbb{H}\setminus\{0\}$, existe um único $\beta \in \mathbb{H}$ tal que $\alpha\beta = 1$. A partir daí, mostre que a *lei do cancelamento* vale em $\mathbb{H}$, i.e., mostre que, se $\alpha, \beta \in \mathbb{H}$ forem tais que $\alpha\beta = 0$, então $\alpha = 0$ ou $\beta = 0$.

10. (Japão.) Seja $\mathcal{P}$ um pentágono cujos lados e diagonais medem, em alguma ordem, $l_1, l_2, \ldots, l_{10}$. Se os números $l_1^2, l_2^2, \ldots, l_9^2$ são todos racionais, prove que l_{10}^2 também é racional.

1.2 A forma polar de um número complexo

Dado $z = a + bi \in \mathbb{C}\setminus\{0\}$, seja $\alpha \in [0, 2\pi)$ a menor determinação, em radianos, do ângulo trigonométrico entre o semieixo real positivo e a semirreta que une 0 a z (veja a figura 1.3).

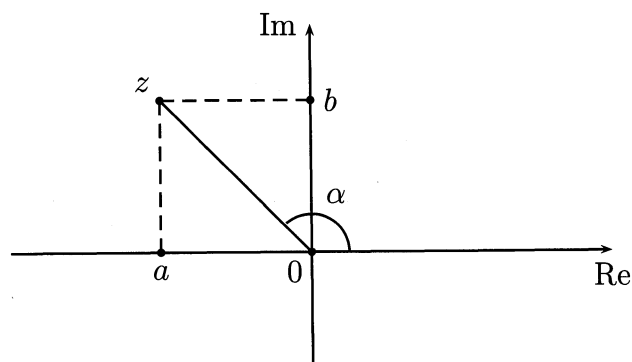



Figura 1.3: forma polar de um número complexo.

Escrevendo

$$z = |z|\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}i\right),$$

segue que

$$\cos\alpha = \frac{a}{\sqrt{a^2+b^2}} \quad \text{e} \quad \operatorname{sen}\alpha = \frac{b}{\sqrt{a^2+b^2}},$$

de maneira que

$$z = |z|(\cos\alpha + i\operatorname{sen}\alpha). \tag{1.12}$$

Como $\operatorname{sen}(\alpha + 2k\pi) = \operatorname{sen}\alpha$ e $\cos(\alpha + 2k\pi) = \cos\alpha$ para todo $k \in \mathbb{Z}$, a igualdade (1.12) ainda vale com $\alpha + 2k\pi$ no lugar de α. Por essa razão, diremos doravante que os números da forma $\alpha + 2k\pi$, com $k \in \mathbb{Z}$, são os **argumentos** do complexo não nulo z e que α é o **argumento principal** de z. Ademais, sendo α um argumento qualquer de z, denominaremos a representação (1.12) de **forma polar** (ou **trigonométrica**) de z. Veja, ainda, que

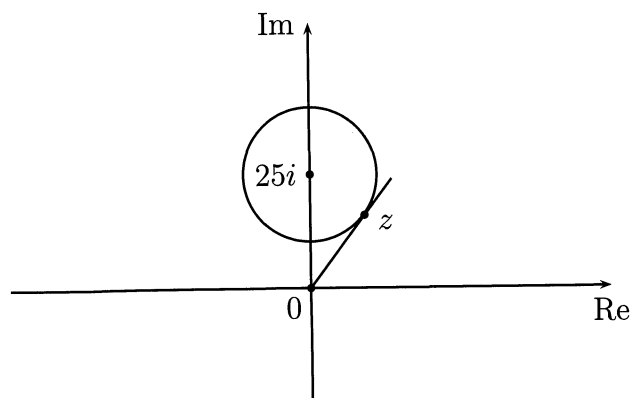
$$|\cos\alpha + i\operatorname{sen}\alpha| = 1, \tag{1.13}$$

para todo $\alpha \in \mathbb{R}$. Também doravante, denotaremos o complexo $\cos\alpha + i\operatorname{sen}\alpha$ simplesmente por $\operatorname{cis}\alpha$. Assim, sendo α um argumento de $z \in \mathbb{C}$, segue de (1.12) que

$$z = |z|\operatorname{cis}\alpha.$$

O exemplo a seguir traz um uso interessante, ainda que elementar, da noção de argumento de um número complexo.

Exemplo 1.5. *Dentre todos os complexos z tais que $|z - 25i| \leq 15$, obtenha o de menor argumento principal.*

Solução. Os complexos satisfazendo a condição do enunciado são aqueles situados sobre o disco fechado de centro $25i$ e raio 15;

destes, o de menor argumento principal é aquele $z \in \mathbb{C}$ tal que a semirreta de origem 0 e que passa por z tangencia tal círculo no primeiro quadrante cartesiano.

Como o raio do círculo é 15, o teorema de Pitágoras, aplicado ao triângulo retângulo de vértices $25i$, z e 0, nos dá $|z| = 20$. Agora, sendo $z = a+bi$, temos que a é igual à altura desse triângulo retângulo relativa à hipotenusa; portanto, as relações métricas em triângulos retângulos (proposição 4.9 de [11]) garantem que $25a = 15 \cdot 20$, de onde segue que $a = 12$. Como $|z| = 20$, temos que

$$20^2 = |z|^2 = a^2 + b^2 = 12^2 + b^2$$

e, daí, $b = 16$. Logo, $z = 12 + 16i$. □

A fórmula (1.14) a seguir, conhecida como a **primeira fórmula de de Moivre**[4], estabelece as vantagens computacionais da representação polar de números complexos.

Proposição 1.6 (de Moivre). *Se $z = |z| \operatorname{cis} \alpha$ é um complexo não nulo e $n \in \mathbb{Z}$, então*

$$z^n = |z|^n \operatorname{cis}(n\alpha). \tag{1.14}$$

[4] Após Abraham de Moivre, matemático francês do século XVIII.

Prova. O caso $n = 0$ é trivial. Supondo que tenhamos provado a fórmula para $n > 0$, mostremos sua validade para $n < 0$. Para tanto, seja $n = -m$, com $m \in \mathbb{N}$. Dado $\theta \in \mathbb{R}$, segue do item (d) do lema 1.1 e de $|\operatorname{cis} \theta| = 1$ que

$$\begin{aligned}(\operatorname{cis} \theta)^{-1} &= \overline{\operatorname{cis} \theta} = \overline{\cos \theta + i \operatorname{sen} \theta} = \cos \theta - i \operatorname{sen} \theta \\ &= \cos(-\theta) + i \operatorname{sen}(-\theta) = \operatorname{cis}(-\theta).\end{aligned} \tag{1.15}$$

Portanto, como estamos assumindo a validade de (1.14) com m no lugar de n, segue que

$$\begin{aligned}z^n &= z^{-m} = (|z| \operatorname{cis} \alpha)^{-m} = |z|^{-m}(\operatorname{cis}(m\alpha))^{-1} \\ &= |z|^n \operatorname{cis}(-m\alpha) = |z|^n \operatorname{cis}(n\alpha).\end{aligned}$$

Para o caso $n > 0$, façamos indução sobre n, sendo o caso $n = 1$ trivial. Supondo o resultado válido para um certo $n \in \mathbb{N}$, temos

$$\begin{aligned}z^{n+1} &= z \cdot z^n = |z| \operatorname{cis} \alpha \cdot |z|^n \operatorname{cis}(n\alpha) \\ &= |z|^{n+1} \operatorname{cis} \alpha \cdot \operatorname{cis}(n\alpha),\end{aligned}$$

e basta mostrarmos que $\operatorname{cis} \alpha \cdot \operatorname{cis}(n\alpha) = \operatorname{cis}(n+1)\alpha$, i.e., que

$$(\cos \alpha + i \operatorname{sen} \alpha)(\cos(n\alpha) + i \operatorname{sen}(n\alpha)) = \cos(n+1)\alpha + i \operatorname{sen}(n+1)\alpha.$$

Mas, esta última igualdade é imediata a partir das fórmulas trigonométricas de adição de arcos (proposição 7.18 de [11]). □

O corolário a seguir fornece a interpretação geométrica usual para a multiplicação de números complexos, um dos quais de módulo 1. Para o caso geral, referimos ao leitor o problema 1.

Corolário 1.7. *Sejam α um real dado e $z \in \mathbb{C} \setminus \{0\}$. Se $\mathbf{u}$ é o vetor de origem 0 e extremidade z, então o ponto do plano complexo que representa $(\operatorname{cis} \alpha) \cdot z$ é a extremidade do vetor obtido mediante a* rotação trigonométrica[5] *de $\mathbf{u}$ pelo ângulo α (veja a figura 1.4).*

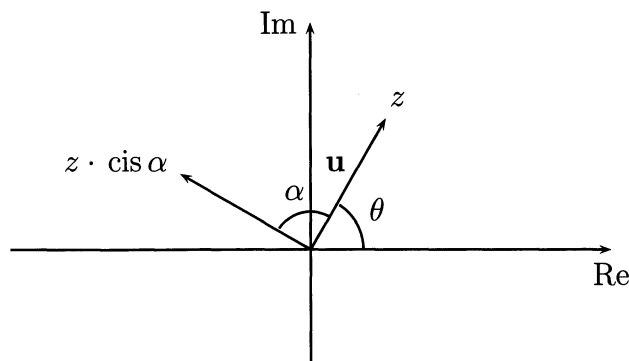



Figura 1.4: interpretando geometricamente a multiplicação por $\operatorname{cis}\alpha$.

Prova. Sendo $z = |z| \operatorname{cis}\theta$, temos da primeira fórmula de de Moivre que

$$z \cdot \operatorname{cis}\alpha = |z| \operatorname{cis}\theta \cdot \operatorname{cis}\alpha = |z| \operatorname{cis}(\theta + \alpha).$$

Mas, este último complexo é exatamente a extremidade do vetor obtido pela rotação de **u** do ângulo α, no sentido trigonométrico. □

Corolário 1.8. *Se $z = |z| \operatorname{cis}\alpha$ e $w = |w| \operatorname{cis}\beta$ são complexos não nulos quaisquer, então*

$$zw = |zw| \operatorname{cis}(\alpha + \beta) \quad e \quad \frac{z}{w} = \frac{|z|}{|w|} \cdot \operatorname{cis}(\alpha - \beta).$$

Em particular, $\alpha + \beta$ (resp. $\alpha - \beta$) é a medida em radianos de um argumento para zw (resp. z/w).

Prova. Façamos a prova para $\frac{z}{w}$, sendo o outro caso totalmente análogo. Para tanto, basta ver que, por (1.15),

$$\frac{z}{w} = |z| \operatorname{cis}\alpha \cdot |w|^{-1} \operatorname{cis}(-\beta) = \frac{|z|}{|w|} \cdot \operatorname{cis}(\alpha - \beta).$$

[5]Quer dizer, *giramos* **u** de um ângulo de medida α radianos, no sentido anti-horário se $\alpha > 0$ e no sentido horário se $\alpha < 0$.

□

Dados $n \in \mathbb{N}$ e $z \in \mathbb{C} \setminus \{0\}$, entendemos por uma **raiz n−ésima** de z um complexo w tais que $w^n = z$. Contrariamente ao que ocorre com números reais, cada complexo não nulo z tem exatamente n raízes n−ésimas, as quais denotaremos genericamente por $\sqrt[n]{z}$. A fórmula (1.16) a seguir, conhecida como a **segunda fórmula de de Moivre**, nos ensina a calculá-las.

Proposição 1.9 (de Moivre). *Se $z = |z| \operatorname{cis}\alpha$ é um complexo não nulo e n é um inteiro positivo qualquer, então há exatamente n valores complexos distintos para a raiz n−ésima de z. Ademais, tais valores são dados por*

$$\sqrt[n]{|z|} \cdot \operatorname{cis}\left(\frac{\alpha + 2k\pi}{n}\right); \quad 0 \le k < n,\ k \in \mathbb{N}, \tag{1.16}$$

onde $\sqrt[n]{|z|}$ é a raiz real positiva de $|z|$.

Prova. Se $w = r \operatorname{cis}\theta$, então

$$\begin{aligned} w^n = z &\Leftrightarrow (r \operatorname{cis}\theta)^n = |z| \operatorname{cis}\alpha \\ &\Leftrightarrow r^n \operatorname{cis}(n\theta) = |z| \operatorname{cis}\alpha \\ &\Leftrightarrow r^n = |z| \text{ e } n\theta = \alpha + 2k\pi,\ \exists\, k \in \mathbb{Z}. \end{aligned}$$

Estas últimas duas igualdades ocorrem se, e só se, $r = \sqrt[n]{|z|}$ e $\theta = \frac{\alpha + 2k\pi}{n}$, para algum $k \in \mathbb{Z}$. Portanto, haverá tantas raízes n−ésimas de z distintas quantos forem os números $\operatorname{cis}\left(\frac{\alpha+2k\pi}{n}\right)$ distintos. Mas é fácil ver que

$$\operatorname{cis}\left(\frac{\alpha + 2k\pi}{n}\right) = \operatorname{cis}\left(\frac{\alpha + 2(k+n)\pi}{n}\right)$$

e

$$\operatorname{cis}\left(\frac{\alpha + 2k\pi}{n}\right) \ne \operatorname{cis}\left(\frac{\alpha + 2l\pi}{n}\right)$$

para $0 \le k < l < n$, de maneira que basta considerarmos os inteiros k tais que $0 \le k < n$. □

Em que pese a fórmula acima, vale frisar que nem sempre ela se constitui na melhor maneira de calcularmos as raízes de um certo índice de um número complexo; isto porque nem sempre a forma trigonométrica de complexo é efetivamente útil para cálculos. Veja o que ocorre no exemplo a seguir.

Exemplo 1.10. *Calcule as raízes quadradas de* $7 + 24i$.

Solução. Se tentarmos utilizar a segunda fórmula de de Moivre, teremos de começar observando que

$$7 + 24i = 25(\cos\alpha + i \operatorname{sen}\alpha),$$

onde $\alpha = \operatorname{arctg}\frac{24}{7}$. Mas, como tal arco não é um arco notável, os cálculos trigonométricos que teremos de fazer para utilizar a segunda fórmula de de Moivre serão mais trabalhosos do que a utilização direta da definição de raiz quadrada de um número complexo. Senão, vejamos:

Seja $7 + 24i = (a + bi)^2$, com $a, b \in \mathbb{R}$. Desenvolvendo $(a + bi)^2$ e igualando em seguida as partes real e imaginária, obtemos o sistema de equações

$$\begin{cases} a^2 - b^2 = 7 \\ ab = 12 \end{cases}.$$

Elevando a segunda equação ao quadrado e substituindo $a^2 = b^2 + 7$ no resultado, chegamos à equação $(b^2 + 7)b^2 = 144$, de sorte que $b^2 = 9$. Mas, como $ab = 12 > 0$, concluímos que a e b devem ter sinais iguais e, a partir daí, que os possíveis pares (a, b) são $(a, b) = (3, 4)$ ou $(-3, -4)$. Logo, as raízes quadradas procuradas são os números complexos $\pm(3 + 4i)$. □

Como caso particular importante da discussão sobre raízes de números complexos, dizemos que o número complexo ω é uma **raiz da unidade** se existir um natural n tal que $\omega^n = 1$. Neste caso, ω é denominado uma **raiz n−ésima da unidade**.

Como $1 = \operatorname{cis} 0$, a segunda fórmula de de Moivre nos diz que há precisamente n raízes n−ésimas distintas da unidade, as quais são dadas por

$$\omega_k = \operatorname{cis}\left(\frac{2k\pi}{n}\right);\ 0 \leq k < n,\ k \in \mathbb{Z}. \tag{1.17}$$

Denotando $\omega = \operatorname{cis}\frac{2\pi}{n}$, segue imediatamente de (1.17) e da primeira fórmula de de Moivre que as raízes n−ésimas da unidade são os números complexos

$$1, \omega, \ldots, \omega^{n-1}. \tag{1.18}$$

À guisa de fixação, vejamos dois exemplos.

Exemplo 1.11. *Dado* $n \in \mathbb{N}$, *ache, em função de* n, *as soluções da equação* $(z - 1)^n = z^n$.

Solução. Como $z = 0$ não é raiz, a equação equivale a $\left(1 - \frac{1}{z}\right)^n = 1$. Portanto, sendo $\omega = \operatorname{cis}\frac{2\pi}{n}$, segue da discussão acima que $1 - \frac{1}{z}$ é igual a um dos números $\omega, \omega^2, \ldots, \omega^{n-1}$ (note que 1 também não é raiz da equação dada). Como $1 - \frac{1}{z} = \omega^k$ se, e só se, $z = \frac{1}{1-\omega^k}$, segue que z é igual a um dos números complexos

$$\frac{1}{1-\omega}, \frac{1}{1-\omega^2}, \ldots, \frac{1}{1-\omega^{n-1}}.$$

□

Para o que segue, recordemos (conforme discussão que precede o problema 6, página 12) que uma sequência de números complexos é uma função $f : \mathbb{N} \to \mathbb{C}$, a qual será, o mais das vezes, denotada simplesmente por $(z_n)_{n\geq 1}$, onde $z_n = f(n)$. Isto posto, observamos que a demonstração da fórmula para a soma dos n primeiros termos de uma PG de números reais e razão diferente de 0 e 1 é válida, *ipsis literis*, para uma *PG de números complexos*, i.e., uma sequência $(z_n)_{n\geq 1}$ de complexos, tal que $z_{k+1} = qz_k$ para todo $k \geq 1$, onde $q \in \mathbb{C} \setminus \{0, 1\}$. Portanto, podemos enunciar o resultado auxiliar a seguir.

Lema 1.12. *Para $z \in \mathbb{C} \setminus \{0,1\}$, temos*

$$1 + z + z^2 + \cdots + z^{n-1} = \frac{z^n - 1}{z - 1}.$$

Como corolário do lema acima, note que, se $\omega \neq 1$ é uma raiz $n-$ésima da unidade, então $\omega^n = 1$, de maneira que

$$1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0. \tag{1.19}$$

Utilizaremos a fórmula acima várias vezes em nossas discussões posteriores.

Exemplo 1.13 (IMO). *Use números complexos para provar que*

$$\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = \frac{1}{2}.$$

Prova. Se $\omega = \operatorname{cis}\frac{2\pi}{7}$, uma raiz sétima da unidade, então

$$\begin{aligned}\operatorname{Re}(\omega + \omega^2 + \omega^3) &= \cos\frac{2\pi}{7} + \cos\frac{4\pi}{7} + \cos\frac{6\pi}{7}\\ &= \cos\frac{2\pi}{7} - \cos\frac{3\pi}{7} - \cos\frac{\pi}{7}.\end{aligned}$$

Por outro lado, como $\omega^k \cdot \omega^{7-k} = 1$ e $|\omega^k| = 1$, segue do item (d) do lema 1.1 que

$$\omega^{7-k} = (\omega^k)^{-1} = \overline{\omega^k}.$$

Portanto, $\overline{\omega + \omega^2 + \omega^3} = \omega^6 + \omega^5 + \omega^4$ e, daí,

$$\operatorname{Re}(\omega + \omega^2 + \omega^3) = \operatorname{Re}(\omega^6 + \omega^5 + \omega^4). \tag{1.20}$$

Por fim, segue de (1.19) que

$$\omega + \omega^2 + \cdots + \omega^6 = -1;$$

daí, tomando partes reais e utilizando (1.20), obtemos

$$2\operatorname{Re}(\omega + \omega^2 + \omega^3) = \operatorname{Re}(\omega + \omega^2 + \omega^3) + \operatorname{Re}(\omega^6 + \omega^5 + \omega^4) = -1$$

e segue, de (1.20), que

$$\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = -\operatorname{Re}(\omega + \omega^2 + \omega^3) = \frac{1}{2}.$$

□

O próximo resultado usa a segunda fórmula de de Moivre para dar uma bela interpretação geométrica para as raízes $n-$ésimas de um complexo não nulo.

Proposição 1.14. *Se z é um complexo não nulo e $n > 2$ é um natural, então as raízes $n-$ésimas de z são os vértices de um $n-$ágono regular centrado na origem do plano complexo.*

Prova. Sendo α um argumento de z, segue da segunda fórmula de de Moivre que as raízes $n-$ésimas de z são os complexos $z_0, z_1, \ldots, z_{n-1}$ tais que

$$z_k = \sqrt[n]{|z|} \cdot \operatorname{cis}\left(\frac{\alpha + 2k\pi}{n}\right),$$

para $0 \leq k < n$.

A partir de (1.13), obtemos

$$|z_k| = \sqrt[n]{|z|}\left|\operatorname{cis}\left(\frac{\alpha + 2k\pi}{n}\right)\right| = \sqrt[n]{|z|},$$

de sorte que os pontos z_k estão todos situados sobre o círculo de centro 0 e raio $\sqrt[n]{|z|}$ do plano complexo. Por outro lado, segue do corolário 1.8 que

$$\frac{z_{k+1}}{z_k} = \operatorname{cis}\left(\frac{2\pi}{n}\right),$$

para $0 \leq k < n$. Então, sendo $\mathbf{u}_k$ o vetor de origem 0 e extremidade z_k, segue do corolário 1.7 que o ângulo entre $\mathbf{u}_k$ e $\mathbf{u}_{k+1}$, medido em radianos e no sentido anti-horário, é, para $0 \leq k < n$, igual a $\frac{2\pi}{n}$.

A proposição decorre imediatamente desses dois fatos. □

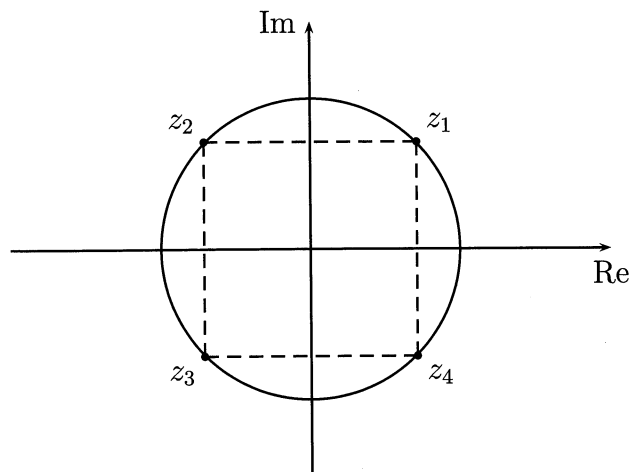



Figura 1.5: disposição geométrica de raízes quartas de -1.

Exemplo 1.15. *Na figura 1.5, representamos, no plano complexo, as raízes quartas de* -1. *Observe que* $z_1 = \sqrt{|-1|}\operatorname{cis}\frac{\pi}{4} = \frac{1+i}{\sqrt{2}}$.

O corolário a seguir isola uma consequência importante do resultado anterior.

Corolário 1.16. *As raízes $n-$ésimas da unidade se dispõem, no plano complexo, como os vértices do polígono regular de n lados, inscrito no círculo de raio* 1 *centrado na origem e tendo o número* 1 *como um de seus vértices.*

Exemplo 1.17. *Na figura 1.6, temos* $\omega = \operatorname{cis}\frac{2\pi}{6} = \frac{1+i\sqrt{3}}{2}$, *de sorte que os números complexos* $1, \omega, \ldots, \omega^5$ *são as raízes sextas da unidade. Os números* 1, ω^2 *e* ω^4 *são as raízes cúbicas da unidade, ao passo que os números* ω, $\omega^3 = -1$ *e* ω^5 *são as raízes cúbicas de* -1.

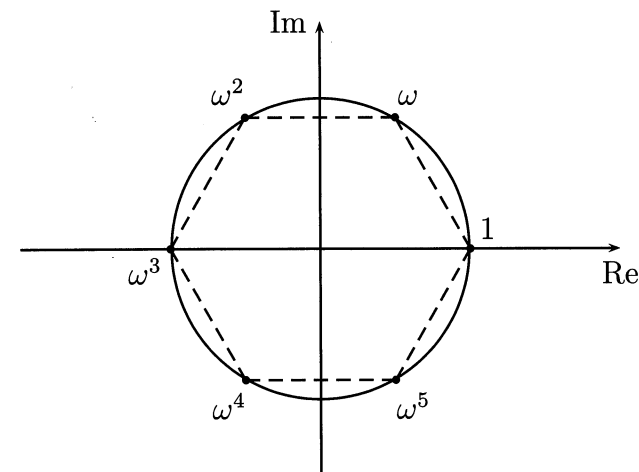



Figura 1.6: raízes sextas da unidade.

Problemas – Seção 1.2

1. Para $r \in \mathbb{R} \setminus \{0\}$, definimos a **homotetia** de **centro** 0 e **razão** r como a função $H_r : \mathbb{C} \to \mathbb{C}$, tal que $H_r(z) = rz$, para todo $z \in \mathbb{C}$. Para $\theta \in \mathbb{R} \setminus \{0\}$, definimos a **rotação** de **centro** 0 e **ângulo** θ como a função $R_\theta : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$, tal que $R_\theta(z) = (\operatorname{cis}\theta)z$, para todo $z \in \mathbb{C} \setminus \{0\}$.

   (a) Seja $\mathbf{u}$ o vetor de origem 0 e extremidade z. Se $w = H_r(z)$, prove que o vetor de origem 0 e extremidade w é $r\mathbf{u}$.

   (b) Se $w = r\operatorname{cis}\theta$ é um complexo não nulo, prove que, para todo $z \in \mathbb{C} \setminus \{0\}$, temos
   $$wz = H_r \circ R_\theta(z).$$

2. (OCM.) Seja ω um número complexo tal que $\omega^2 + \omega + 1 = 0$.

Calcule o valor do produto

$$\prod_{k=1}^{27}\left(\omega^k+\frac{1}{\omega^k}\right).$$

3. Seja n um natural múltiplo de 3. Calcule o valor de $(1+\sqrt{3}i)^n-(1-\sqrt{3}i)^n$.

4. Resolva em $\mathbb{C}$ o sistema de equações

$$\begin{cases} |z_1|=|z_2|=|z_3|=1 \\ z_1+z_2+z_3=0 \\ z_1z_2z_3=1 \end{cases}.$$

5. Encontre, em função de $n\in\mathbb{N}$, as soluções da equação

$$(1+z)^{2n}+(1-z)^{2n}=0.$$

6. Mostre que todas as raízes da equação $(z-1)^5=32(z+1)^5$ estão situadas sobre o círculo do plano complexo de raio $\frac{4}{3}$ e centro $-\frac{5}{3}$.

7. (Irlanda.) Para cada $n\in\mathbb{N}$, defina $a_n=n^2+n+1$. Dado $k\in\mathbb{N}$, prove que existe $m\in\mathbb{N}$ tal que $a_{k-1}a_k=a_m$.

8. (Romênia.) Sejam $p,q\in\mathbb{C}$, com $q\neq 0$, tais que a equação $x^2+px+q^2=0$ tem raízes de módulos iguais. Prove que $\frac{p}{q}\in\mathbb{R}$.

9. Sejam z_1, z_2 e z_3 números complexos não todos nulos. Prove que z_1, z_2 e z_3 são os vértices de um triângulo equilátero no plano complexo se, e só se,

$$z_1^2+z_2^2+z_3^2=z_1z_2+z_2z_3+z_3z_1.$$

10. Dado $n>2$ inteiro, use números complexos para provar que

$$\sum_{k=0}^{n-1}\cos\frac{2k\pi}{n}=\sum_{k=0}^{n-1}\operatorname{sen}\frac{2k\pi}{n}=0.$$

11. Dados $n>2$ inteiro e $\alpha\in\mathbb{R}$, use números complexos para calcular cada uma das somas abaixo em função de n e α:

    (a) $\operatorname{sen}\alpha+\operatorname{sen}(2\alpha)+\operatorname{sen}(3\alpha)+\cdots+\operatorname{sen}(n\alpha)$.

    (b) $\operatorname{sen}^2\alpha+\operatorname{sen}^2(2\alpha)+\operatorname{sen}^2(3\alpha)+\cdots+\operatorname{sen}^2(n\alpha)$.

12. Dê exemplo de um conjunto infinito $\mathcal{T}\subset\mathbb{C}$ satisfazendo as seguintes condições:

    (a) Para todo $z\in\mathcal{T}$ existe $n\in\mathbb{N}$ tal que $z^n=1$.

    (b) Para todos $z,w\in\mathcal{T}$, temos $zw\in\mathcal{T}$.

13. (Croácia.) Sejam n um natural dado e A um conjunto de n números complexos não nulos, tendo a seguinte propriedade: se quaisquer dois de seus elementos (não necessariamente distintos) forem multiplicados, obtemos outro elemento do conjunto. Ache todos os conjuntos A possíveis.

14. Seja $g:\mathbb{C}\to\mathbb{C}$ uma função dada e $\omega=\operatorname{cis}\frac{2\pi}{3}$. Para cada número complexo dado a, prove que há uma única função $f:\mathbb{C}\to\mathbb{C}$ tal que

$$f(z)+f(\omega z+a)=g(z),\forall\, z\in\mathbb{C}.$$

CAPÍTULO 2

Polinômios

De um ponto de vista mais *algébrico*, funções polinomiais reais podem ser encaradas como *polinômios* de coeficientes reais. Conforme veremos a partir deste capítulo, um tal ponto de vista resulta muitíssimo frutífero no estudo de polinômios, não somente os de coeficientes reais, mas também aqueles com coeficientes racionais ou, mais geralmente, complexos. Nesse sentido, em tudo o que segue, sempre que uma propriedade for válida para polinômios com coeficientes em um qualquer dos conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, escreveremos simplesmente $\mathbb{K}$ para denotar tais conjuntos, salvo menção explícita em contrário. Nosso propósito é, pois, desenvolver os aspectos algébricos elementares da teoria dos polinômios sobre $\mathbb{K}$.[1]

[1]Para os que já estudaram um pouco de Estruturas Algébricas, frisamos que $\mathbb{K}$ poderia denotar um corpo qualquer de característica 0. De fato, a restrição de $\mathbb{K}$ a $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ é meramente psicológia, tendo o intuito de tornar o mais elementar possível a discussão subsequente.

2.1 Definições e propriedades básicas

Colecionamos, nesta seção, as definições e notações básicas sobre polinômios, as quais serão fundamentais para os desenvolvimentos subsequentes da teoria.

Definição 2.1. *Uma sequência $(a_0, a_1, a_2, \ldots)$ de elementos de $\mathbb{K}$ é dita* quase toda nula *se existir $n \geq -1$ tal que*

$$a_{n+1} = a_{n+2} = a_{n+3} = \cdots = 0.$$

Em palavras, uma sequência $(a_0, a_1, a_2, \ldots)$ é quase toda nula se todos os seus termos, de uma certa posição em diante, forem iguais a zero. Por exemplo, as sequências

$$(0, 0, 0, 0, 0, 0, \ldots) \text{ e } (1, 2, 3, \ldots, n, 0, 0, 0, \ldots)$$

são quase todas nulas; por outro lado, a sequência $(1, 0, 1, 0, 1, \ldots)$, com 1's e 0's se alternando indefinidamente, não é quase toda nula.

Definição 2.2. *Um polinômio sobre (ou com coeficientes em) $\mathbb{K}$ é uma* soma formal $f = f(X)$ *do tipo*

$$f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots := \sum_{k \geq 0} a_kX^k, \tag{2.1}$$

onde $(a_0, a_1, a_2, \ldots)$ é uma sequência quase toda nula de elementos de $\mathbb{K}$ e convencionamos $X^0 = 1$ e $X^1 = X$ no somatório acima.

Ainda em relação à definição acima, cumpre observar que X é um símbolo qualquer. Em particular, X não representa uma variável e poderíamos, por exemplo, ter utilizado o símbolo $\square$ em seu lugar. Assumiremos ainda que os polinômios $f(X) = \sum_{k \geq 0} a_kX^k$ e $g(X) = \sum_{k \geq 0} b_kX^k$ sobre $\mathbb{K}$ são **iguais** se, e só se, $a_k = b_k$, para todo $k \geq 0$.

Dado um polinômio $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots$ sobre $\mathbb{K}$, adotamos as seguintes convenções:

i. Os elementos $a_i \in \mathbb{K}$ são denominados os **coeficientes** de f.

ii. Quando $a_i = 0$ omitiremos, sempre que for conveniente, o termo a_iX^i. Em particular, como a sequência $(a_0, a_1, a_2, \ldots)$ é quase toda nula, existe um inteiro $n \geq 0$ para o qual podemos escrever

$$f(X) = \sum_{k=0}^{n} a_kX^k.$$

iii. Quando $a_i = \pm 1$, escreveremos $\pm X^i$ em vez de $(\pm 1)X^i$, para o termo correspondente de f.

iv. O polinômio $0 = 0 + 0X + 0X^2 + \cdots$ é denominado o **polinômio identicamente nulo** sobre $\mathbb{K}$. Sempre que não houver perigo de confusão com $0 \in \mathbb{K}$, denotaremos o polinômio identicamente nulo sobre $\mathbb{K}$ simplesmente por 0.

v. Mais geralmente (e consoante ii.), dado $\alpha \in \mathbb{K}$, denotamos o polinômio $\alpha + 0X + 0X^2 + \cdots$ simplesmente por α e o denominamos o **polinômio constante** α; em cada caso, o contexto deixará claro se estamos nos referindo ao polinômio constante e igual a α ou ao elemento $\alpha \in \mathbb{K}$.

Denotamos por $\mathbb{K}[X]$ o conjunto de todos os polinômios sobre $\mathbb{K}$. Em particular, de posse do item v. acima, convencionamos também que

$$\mathbb{K} \subset \mathbb{K}[X].$$

Por outro lado, as inclusões $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ fornecem as inclusões

$$\mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X].$$

Exemplo 2.3. *Se $f(X) = 1 + X - X^3 + \sqrt{2}X^7$, então $f \notin \mathbb{Q}[X]$ (uma vez que $\sqrt{2} \notin \mathbb{Q}$) mas $f \in \mathbb{R}[X]$. Já a expressão $g = 1 + X + X^2 + X^3 + X^4 + \cdots$ não é um polinômio, uma vez que a sequência $(1, 1, 1, \ldots)$ não é quase toda nula.*

No que segue, vamos definir sobre $\mathbb{K}[X]$ operações

$$\oplus : \mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X] \text{ e } \odot : \mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X],$$

respectivamente denominadas **adição** e **multiplicação**. Para tanto, precisamos inicialmente do seguinte resultado auxiliar.

Lema 2.4. *Se $(a_k)_{k\geq 0}$ e $(b_k)_{k\geq 0}$ são sequências quase todas nulas de elementos de $\mathbb{K}$, então também são quase todas nulas as sequências $(a_k \pm b_k)_{k\geq 0}$ e $(c_k)_{k\geq 0}$, onde*

$$c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}.$$

Prova. Mostremos somente que a sequência $(c_k)_{k\geq 0}$ é quase toda nula, ficando o outro caso como exercício para o leitor (veja o problema 1). Sejam $m, n \in \mathbb{Z}_+$ tais que $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$. Se $k > m + n$ e $i + j = k$, com $i, j \geq 0$, então $i > n$ ou $j > m$, pois, do contrário, teríamos $k = i + j \leq n + m$, o que não é o caso. Mas, como $i > n \Rightarrow a_i = 0$ e $j > m \Rightarrow b_j = 0$, em qualquer caso temos $a_i b_j = 0$, de sorte que

$$c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j = 0.$$

□

De posse do lema anterior, podemos finalmente formular as definições das operações de adição e multiplicação de polinômios.

Definição 2.5. *Dados em $\mathbb{K}[X]$ os polinômios*

$$f(X) = \sum_{k\geq 0} a_k X^k \text{ e } g(X) = \sum_{k\geq 0} b_k X^k,$$

a **soma** *e o* **produto** *de f e g, denotados respectivamente por $f \oplus g$ e $f \odot g$, são os polinômios*

$$(f \oplus g)(X) = \sum_{k\geq 0} (a_k + b_k) X^k$$

e

$$(f \odot g)(X) = \sum_{k\geq 0} c_k X^k,$$

onde $c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j$.

Ainda que, em princípio, possa não parecer, a definição do produto de dois polinômios é bastante natural: a fórmula para o coeficiente c_k de $f \odot g$ é necessária se quisermos que valham a distributividade da operação $\odot$ em relação à operação $\oplus$, bem como a regra usual de potenciação $X^m \odot X^n = X^{m+n}$. De fato, se tais propriedades forem válidas, então, calculando o produto

$$(a_0 + a_1 X + a_2 X^2 + \cdots) \odot (b_0 + b_1 X + b_2 X^2 + \cdots)$$

distributivamente, obtemos

$$a_0 b_0 = \sum_{\substack{i+j=0 \\ i,j\geq 0}} a_i b_j$$

para coeficiente de X^0,

$$a_0 b_1 + a_1 b_0 = \sum_{\substack{i+j=1 \\ i,j\geq 0}} a_i b_j$$

para coeficiente de X,

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = \sum_{\substack{i+j=2 \\ i,j\geq 0}} a_i b_j$$

para coeficiente de X^2 e assim por diante.

De fato, não é difícil nos convencermos (cf. problema 3) de que, conforme foram definidas, as operações de adição e multiplicação de polinômios sobre $\mathbb{K}$ gozam das seguintes propriedades:

i. **Comutatividade**: $f \oplus g = g \oplus f$ e $f \odot g = g \odot f$;

ii. **Associatividade**: $(f \oplus g) \oplus h = f \oplus (g \oplus h)$ e $(f \odot g) \odot h = f \odot (g \odot h)$;

iii. **Distributividade**: $f \odot (g \oplus h) = (f \odot g) \oplus (f \odot h)$,

para todos $f, g, h \in \mathbb{K}[X]$.

Exemplo 2.6. *Considere os polinômios de coeficientes reais* $f(X) = 1 + X - \sqrt{2}X^2 - 4X^3$ *e* $g(X) = X + X^2$, *onde, como anteriormente convencionado, omitimos os coeficientes nulos. Então*

$$(f \oplus g)(X) = 1 + 2X + (1 - \sqrt{2})X^2 - 4X^3$$

e

$$\begin{aligned}(f \odot g)(X) &= (1 + X - \sqrt{2}X^2 - 4X^3) \odot (X + X^2)\\ &= [1 \odot (X + X^2)] \oplus [X \odot (X + X^2)] \oplus\\ &\oplus [-\sqrt{2}X^2 \odot (X + X^2)] \oplus [-4X^3 \odot (X + X^2)]\\ &= (X + X^2) \oplus (X^2 + X^3) \oplus (-\sqrt{2}X^3 - \sqrt{2}X^4) \oplus\\ &\quad \oplus (-4X^4 - 4X^5)\\ &= X + 2X^2 + (1 - \sqrt{2})X^3 - (\sqrt{2} + 4)X^4 - 4X^5.\end{aligned}$$

A discussão acima deixa claro que podemos relaxar nossas notações, denotando, a partir de agora, as operações de adição e multiplicação de polinômios simplesmente por $+$ e $\cdot$. Assim, sempre que adicionarmos dois polinômios, os sinais $+$ representarão duas operações diferentes: a adição de elementos de $\mathbb{K}$, efetuada sobre os coeficientes dos polinômios em questão, e a adição de elementos de $\mathbb{K}[X]$. No entanto, isto não deve causar confusão, uma vez que o contexto sempre

deixará claro a qual operação o sinal $+$ se refere. Note, ainda, que um comentário análogo é válido para o sinal $\cdot$ de multiplicação.

Observação 2.7. *Todas as definições acima podem ser estendidas, aliás de maneira óbvia, para incluir polinômios de coeficientes* inteiros. *Doravante, sempre que necessário, denotaremos o conjunto de tais polinômios por* $\mathbb{Z}[X]$.

Sendo 0 o polinômio identicamente nulo, temos $f + 0 = 0 + f = 0$ para todo $f \in \mathbb{K}[X]$, i.e, o polinômio identicamente nulo é o **elemento neutro** da adição de polinômios. Por outro lado, dado $f \in \mathbb{K}[X]$, existe um único polinômio $g \in \mathbb{K}[X]$ tal que $f + g = g + f = 0$: de fato, sendo $f(X) = a_0 + a_1X + a_2X^2 + \cdots$, é imediato que

$$g(X) = -a_0 - a_1X - a_2X^2 - \cdots$$

é esse único polinômio, o qual será, doravante, denotado por $-f$. Assim,

$$(-f)(X) = -a_0 - a_1X - a_2X^2 - \cdots$$

e, para $f, g \in \mathbb{K}[X]$, podemos definir a **diferença** $f - g$ entre f e g por $f - g = f + (-g)$.

Para $\alpha \in \mathbb{K}$ e $g(X) = b_0 + b_1X + b_2X^2 + \cdots \in \mathbb{K}[X]$, é imediato verificar que

$$\alpha \cdot g = \alpha b_0 + \alpha b_1X + \alpha b_2X^2 + \cdots;$$

em particular, temos $1 \cdot g = g$ para todo $g \in \mathbb{K}[X]$, de maneira que o polinômio constante 1 é o elemento neutro da multiplicação de polinômios.

Doravante, sempre que não houver perigo de confusão, escreveremos simplesmente fg para denotar o produto $f \cdot g$, de $f, g \in \mathbb{K}[X]$. Em particular, se $\alpha \in \mathbb{K}$, então αf denotará o produto de α, visto como polinômio constante, e f.

A definição a seguir desempenhará papel central ao longo do texto.

Definição 2.8. *Se* $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X] \setminus \{0\}$, *com* $a_n \neq 0$, *dizemos que o inteiro não negativo* n *é o* **grau** *de* f, *e denotamos* $\partial f = n$ (*lê-se* "o grau de f é igual a n").

Veja que só definimos grau para polinômios não identicamente nulos; por outro lado, $\partial f = 0$ para todo polinômio constante $f(X) = \alpha$, com $\alpha \in \mathbb{K} \setminus \{0\}$. Doravante, sempre que nos referirmos a $f \in \mathbb{K}[X] \setminus \{0\}$ escrevendo

$$f(X) = a_nX^n + \cdots + a_1X + a_0$$

suporemos, salvo menção em contrário, que $a_n \neq 0$. Nesse caso, a_n será denominado o **coeficiente líder** de f. Finalmente, f será dito **mônico** quando tiver coeficiente líder 1.

A proposição a seguir estabelece duas propriedades muito importantes da noção de grau de polinômios.

Proposição 2.9. *Para* $f, g \in \mathbb{K}[X] \setminus \{0\}$, *temos:*

(a) $\partial(f + g) \leq \max\{\partial f, \partial g\}$ *se* $f + g \neq 0$.

(b) $fg \neq 0$ *e* $\partial(fg) = \partial f + \partial g$.

Prova. Sejam $\partial f = n$ e $\partial g = m$, com

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \quad \text{e} \quad g(X) = b_0 + b_1X + \cdots + b_mX^m.$$

(a) Se $m \neq n$, podemos supor, sem perda de generalidade, que $m > n$. Então

$$(f + g)(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \cdots + b_mX^m,$$

de forma que $\partial(f + g) = m = \max\{\partial f, \partial g\}$. Se $m = n$ mas $f + g \neq 0$, então

$$(f + g)(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n$$

e há duas possibilidades: $a_n + b_n = 0$ ou $a_n + b_n \neq 0$. No primeiro caso, $\partial(f + g) < n = \max\{\partial f, \partial g\}$. No segundo, $\partial(f + g) = n = \max\{\partial f, \partial g\}$. Em qualquer caso, ainda teremos $\partial(f + g) \leq \max\{\partial f, \partial g\}$.

(b) Seja $fg = c_0 + c_1X + c_2X^2 + \cdots$. Se $k > m + n$, vimos, na prova do lema 2.4, que $c_k = 0$. Portanto, se mostrarmos que $c_{m+n} \neq 0$, seguirá que $fg \neq 0$ e $\partial(fg) = m + n = \partial f + \partial g$. Mas, como $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$, é imediato que

$$c_{m+n} = \sum_{\substack{i+j=m+n \\ i,j \geq 0}} a_ib_j = a_nb_m \neq 0.$$

□

Problemas – Seção 2.1

1. * Se $(a_k)_{k\geq 0}$ e $(b_k)_{k\geq 0}$ são sequências quase todas nulas de elementos de $\mathbb{K}$, mostre que a sequência $(a_k \pm b_k)_{k\geq 0}$ também é quase toda nula.

2. Dado $n \in \mathbb{N}$, execute as seguintes multiplicações de polinômios:

   (a) $(X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$.

   (b) $(X + 1)(X^{n-1} - X^{n-2} + \cdots - X + 1)$, se n for ímpar.

   (c) $(X + 1)(X^2 + 1)(X^4 + 1) \ldots (X^{2^n} + 1)$.

3. * Mostre que as operações de adição e multiplicação de polinômios são comutativas, associativas e que a multiplicação é distributiva em relação à adição.

4. * Mostre que, em $\mathbb{K}[X]$, não há *divisores de zero*. Mais precisamente, mostre que se $f, g \in \mathbb{K}[X]$ são tais que $fg = 0$, então $f = 0$ ou $g = 0$.

5. (Torneio das Cidades.) Encontre pelo menos um polinômio f, de grau 2001, tal que $f(X) + f(1 - X) = 1$.

2.2 O algoritmo da divisão

Já vimos ser possível adicionar, subtrair e multiplicar polinômios, sendo o resultado ainda um polinômio. E quanto à possibilidade de uma operação de *divisão* para polinômios? Bem, nem sempre será possível efetuá-la; em outras palavras, dados polinômios $f, g \in \mathbb{K}[X]$, com $g \neq 0$, nem sempre existirá $h \in \mathbb{K}[X]$ tal que $f = gh$; por exemplo, se $f(X) = X + 1$ e $g(X) = X^2$ então um tal polinômio h não existe, pois, caso existisse, deveríamos ter

$$1 = \partial f = \partial(gh) = \partial g + \partial h = 2 + \partial h$$

e, daí, $\partial h = -1$, o que é um absurdo.

Apesar da discussão do parágrafo anterior, o seguinte análogo da divisão de inteiros, denominado o **algoritmo da divisão para polinômios**, ainda é válido.

Teorema 2.10. *Se $f, g \in \mathbb{K}[X]$, com $g \neq 0$, então existem únicos $q, r \in \mathbb{K}[X]$ tais que*

$$f = gq + r, \text{ com } r = 0 \text{ ou } 0 \leq \partial r < \partial g. \tag{2.2}$$

Prova. Mostremos, inicialmente, que há no máximo um par de polinômios q e r satisfazendo as condições do enunciado. Para tanto, sejam $q_1, q_2, r_1, r_2 \in \mathbb{K}[X]$ tais que

$$f = gq_1 + r_1 = gq_2 + r_2,$$

com $r_i = 0$ ou $0 \leq \partial r_i < \partial g$, para $i = 1, 2$. Então, $g(q_1 - q_2) = r_2 - r_1$ e, se $q_1 \neq q_2$, o problema 4, página 40, garante que $r_1 \neq r_2$. Mas, pela proposição 2.9, temos

$$\begin{aligned} \partial g &\leq \partial g + \partial(q_1 - q_2) = \partial(g(q_1 - q_2)) \\ &= \partial(r_1 - r_2) \leq \max\{\partial r_1, \partial r_2\} < \partial g, \end{aligned}$$

o que é um absurdo. Portanto, $q_1 = q_2$ e, daí, $r_1 = r_2$.

Façamos, agora, a prova da existência de polinômios q e r satisfazendo as condições do enunciado. No que segue, sejam b o coeficiente líder e n o grau de g, e consideremos o seguinte algoritmo:

Algoritmo da divisão para polinômios

1. FAÇA
   - $r \leftarrow f$; $m \leftarrow \partial f$; $q \leftarrow 0$;
   - $a \leftarrow$ COEFICIENTE LÍDER DE r;
2. ENQUANTO $r \neq 0$ OU $\partial r \geq \partial g$ FAÇA
   - $r(X) \leftarrow r(X) - ab^{-1}X^{m-n}g(X)$;
   - $q(X) \leftarrow q(X) + ab^{-1}X^{m-n}$;
   - $m \leftarrow \partial r$
   - $a \leftarrow$ COEFICIENTE LÍDER DE r;
3. LEIA OS VALORES FINAIS DE r E DE q.

Provemos que o algoritmo acima realmente termina após um número finito de repetições do laço ENQUANTO e nos dá, ao final, polinômios q e r como desejado.

Se $r \neq 0$ ou $\partial r \geq \partial g$, então a instrução do laço ENQUANTO troca $r(X)$ pelo polinômio $r(X) - ab^{-1}X^{m-n}g(X)$; tal polinômio, se não for o polinômio nulo, tem grau menor que o de r, uma vez que o

polinômio $ab^{-1}X^{m-n}g(X)$ tem grau m (que é o grau de r antes da execução do laço) e coeficiente líder a (que é o coeficiente líder de r antes da execução do laço). Assim, o algoritmo pára após um número finito de passos.

Após a primeira atribuição, temos

$$f(X) = g(X)q(X) + r(X),$$

uma vez que, no início, $q(X) = 0$ e $r(X) = f(X)$. Suponha, por hipótese de indução, que após uma certa execução do laço ENQUANTO tenhamos $f(X) = g(X)q(X) + r(X)$ e que, nesse momento, $r(X) \neq 0$ e $\partial r \geq \partial g$. Então a próxima execução ocorre e troca $r(X)$ por $r(X) - ab^{-1}X^{m-n}g(X)$ e $q(X)$ por $q(X) + ab^{-1}X^{m-n}$. Como

$$g(X)\left(q(X) + ab^{-1}X^{m-n}\right) + \left(r(X) - ab^{-1}X^{m-n}g(X)\right) \tag{2.3}$$

é igual a $g(X)q(X) + r(X)$, segue da hipótese de indução que, após tal execução, ainda teremos (2.3) igual a $f(X)$. □

Nas notações do algoritmo da divisão para polinômios, dizemos que (o valor final de) q é o **quociente** e (o valor final de) r é o **resto** da divisão de f por g. Ademais, quando $r = 0$, dizemos que f é **divisível** por g ou, ainda, que g **divide** f, e denotamos $g \mid f$.

Observação 2.11. *Como o leitor pode facilmente verificar repassando a discussão acima, o algoritmo da divisão ainda é válido para polinômios em $\mathbb{Z}[X]$, contanto que o coeficiente líder do polinômio divisor seja ± 1. Mais precisamente, se $f, g \in \mathbb{Z}[X]$, onde $g \neq 0$ tem coeficiente líder ± 1, então q e r também têm coeficientes inteiros. No que segue, usaremos esta observação sem maiores comentários.*

Vejamos como o algoritmo da divisão se comporta num exemplo particular. Considere o problema de dividir $f(X) = X^4 - 2X^2 + 5X + 7$ por $g(X) = 3X^2 + 1$ em $\mathbb{Q}[X]$. Iniciamos o algoritmo armazenando os valores $b = 3$ e $n = 2$. Ao segui-lo, temos os seguintes passos:

1. Fazemos as atribuições $r(X) = X^4 - 2X^2 + 5X + 7$; $m = 4$; $q(X) = 0$; $a = 1$.

2. Como nem $r(X) = 0$ nem $m = 4 < n = 2$, trocamos $r(X)$ por
$$\begin{aligned} r(X) - ab^{-1}X^{m-n}g(X) &= \\ &= X^4 - 2X^2 + 5X + 7 - \frac{1}{3}X^{4-2}(3X^2+1) \\ &= -\frac{7}{3}X^2 + 5X + 7, \end{aligned}$$
m por 2, $q(X)$ por
$$q(X) + ab^{-1}X^{m-n} = 0 + \frac{1}{3}X^{4-2} = \frac{1}{3}X^2$$
e a por $-\frac{7}{3}$.

3. Como ainda não temos nem $r(X) = 0$ nem $m = 2 < n = 2$, trocamos $r(X)$ por
$$\begin{aligned} r(X) - ab^{-1}X^{m-n}g(X) &= \\ &= -\frac{7}{3}X^2 + 5X + 7 + \frac{7/3}{3}X^{2-2}(3X^2+1) \\ &= 5X + \frac{70}{9}, \end{aligned}$$
m por 1, $q(X)$ por
$$q(X) + ab^{-1}X^{m-n} = \frac{1}{3}X^2 + \frac{-7/3}{3}X^{2-2} = \frac{1}{3}X^2 - \frac{7}{9}$$
e a por $\frac{1}{3}$.

4. Agora, ainda temos $r(X) \neq 0$, mas $m = 1 < n = 2$, de modo que não mais voltamos para o início do loop. Simplesmente lemos
$$r(X) = 5X + \frac{70}{9} \quad \text{e} \quad q(X) = \frac{1}{3}X^2 - \frac{7}{9}.$$

Podemos esquematizar o procedimento acima na tabela abaixo, ao longo da qual você deve identificar cada uma das passagens acima:

Algoritmo da divisão para polinômios

X^4	$-2X^2$	$+5X$	$+7$	$3X^2+1$
$-X^4$	$-1/3X^2$			$1/3X^2$
	$-7/3X^2$	$+5X$	$+7$	$1/3X^2-7/9$
	$7/3X^2$		$+7/9$	
		$5X$	$+70/9$	

Problemas – Seção 2.2

1. Se $n \in \mathbb{N}$, encontre o resto da divisão do polinômio $(X^2+X+1)^n$ pelo polinômio $X^2 - X + 1$.
2. Dados $m, n \in \mathbb{N}$, com $m > n$, encontre o resto da divisão de $X^{2^m} + 1$ por $X^{2^n} + 1$.
3. Ao dividirmos um polinômio $f \in \mathbb{Q}[X]$ por $X+2$, obtemos resto -1; ao dividirmos f por $X - 2$, obtemos resto 3. Encontre o resto da divisão de f por $X^2 - 4$.
4. Um polinômio $f \in \mathbb{R}[X]$ deixa resto 4 quando dividido por $X+1$ e resto $2X+3$ quando dividido por X^2+1. Obtenha o resto de sua divisão por $(X+1)(X^2+1)$.

CAPÍTULO 3

Raízes de Polinômios

Na exposição que fizemos até agora da teoria de polinômios não tivemos, em momento algum, a intenção de *substituir* X por um número. De outra forma, até o presente momento, polinômios têm sido para nós meramente *expressões formais* com as quais aprendemos a operar. Nesse sentido, a **indeterminada** X é um símbolo sem significado aritmético, e observamos uma vez mais que poderíamos tê-lo substituído pelo símbolo $\square$, por exemplo, sem problema algum.

Remediamos o estado de coisas descrito acima neste capítulo, onde introduzimos o conceito de raiz de um polinômio e de função polinomial associada a um polinômio. Dentre os vários resultados importantes discutidos, destacamos a apresentação de uma demonstração completa do teorema fundamental da álgebra. Outros pontos dignos de nota são a discussão do critério de pesquisa de raízes racionais de polinômios de coeficientes inteiros e a utilização de raízes da unidade como marcadores de posição em certos problemas combinatórios.

3.1 Raízes de polinômios

Para continuar nosso estudo de polinômios, é conveniente considerar a *função polinomial* associada a um polinômio.

Definição 3.1. *Para* $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{K}[X]$, *a* **função polinomial** *associada a* f *é a função* $\tilde{f} : \mathbb{K} \to \mathbb{K}$ *dada, para* $x \in \mathbb{K}$, *por*

$$\tilde{f}(x) = a_nx^n + \cdots + a_1x + a_0.$$

Quando $f(X) = c$, note que a função polinomial associada $\tilde{f}$ será a função constante $\tilde{f}(x) = c$, para todo $x \in \mathbb{K}$, justificando o nome *constante* imputado anteriormente a um polinômio de grau 0.

Definição 3.2. *Seja* $f \in \mathbb{K}[X]$ *um polinômio, com função polinomial associada* $\tilde{f} : \mathbb{K} \to \mathbb{K}$. *Um elemento* $\alpha \in \mathbb{K}$ *é uma* **raiz** *de* f *se* $\tilde{f}(\alpha) = 0$.

Por exemplo, se $f(X) = X + 1 \in \mathbb{C}[X]$, é fácil ver que $x = -1$ é a única raiz de f em $\mathbb{C}$. De fato, a função polinomial associada a f é

$$\begin{array}{rcl} \tilde{f} : \mathbb{C} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & x + 1 \end{array},$$

de sorte que $\tilde{f}(x) = 0$ se, e só se, $x = -1$.

A proposição a seguir é conhecida como o **teste da raiz**.

Proposição 3.3. *Se* $f \in \mathbb{K}[X] \setminus \{0\}$ *e* $\alpha \in \mathbb{K}$, *então:*

(a) α *é raiz de* f *se, e só se,* $(X - \alpha) \mid f(X)$ *em* $\mathbb{K}[X]$.

(b) Se α *for raiz de* f, *então existe um maior inteiro positivo* m *tal que* $(X - \alpha)^m$ *divide* f. *Ademais, sendo* $f(X) = (X - \alpha)^m q(X)$, *com* $q \in \mathbb{K}[X]$, *tem-se* $\tilde{q}(\alpha) \neq 0$, *onde* $\tilde{q} : \mathbb{K} \to \mathbb{K}$ *é a função polinomial associada a* q.

(c) Se $\alpha_1, \ldots, \alpha_k$ *forem raízes duas a duas distintas de* f, *então o polinômio* $(X - \alpha_1) \cdots (X - \alpha_k)$ *divide* $f(X)$ *em* $\mathbb{K}[X]$.

Prova.

(a) Segue do algoritmo da divisão a existência de polinômios $q, r \in \mathbb{K}[X]$ tais que

$$f(X) = (X - \alpha)q(X) + r(X),$$

com $r = 0$ ou $0 \leq \partial r < \partial(X - \alpha) = 1$. Portanto, $r(X) = c$, um polinômio constante. Por outro lado, sendo $\tilde{f}$ e $\tilde{q}$ as funções polinomiais respectivamente associadas a f e q, segue da igualdade acima que

$$\tilde{f}(\alpha) = (\alpha - \alpha)\tilde{q}(\alpha) + c = c,$$

i.e., $f(X) = (X - \alpha)q(X) + \tilde{f}(\alpha)$. Assim,

$$\alpha \text{ é raiz de } f \Leftrightarrow \tilde{f}(\alpha) = 0 \Leftrightarrow f(X) = (X - \alpha)q(X).$$

(b) Se $m > \partial f$, então $(X - \alpha)^m \nmid f(X)$, uma vez que $\partial(X - \alpha)^m = m > \partial f$. Daí e do item (a), existe um maior inteiro positivo m tal que $(X - \alpha)^m \mid f(X)$, digamos $f(X) = (X - \alpha)^m q(X)$. Passando para funções polinomiais, obtemos, a partir daí, a igualdade

$$\tilde{f}(x) = (x - \alpha)^m \tilde{q}(x), \ \forall\, x \in \mathbb{K};$$

se $\tilde{q}(\alpha) = 0$, seguiria de (a) que $q(X) = (X - \alpha)q_1(X)$, para algum polinômio $q_1 \in \mathbb{K}[X]$. Mas aí, teríamos

$$f(X) = (X - \alpha)^{m+1} q_1(X),$$

contrariando a maximalidade de m.

(c) Façamos a prova deste item para o caso $k = 2$ (a prova do caso geral é inteiramente análoga). Como α_1 é raiz de f, pelo item (a) existe um polinômio $g \in \mathbb{K}[X]$ tal que $f(X) = (X - \alpha_1)g(X)$. Seja

$\tilde{g}$ a função polinomial associada ao polinômio g. Como $\alpha_1 \neq \alpha_2$ e α_2 também é raiz de f, segue da última igualdade que

$$0 = \tilde{f}(\alpha_2) = (\alpha_2 - \alpha_1)\tilde{g}(\alpha_2),$$

e α_2 é raiz de g. Daí, novamente pelo item (a), existe um polinômio $h \in \mathbb{K}[X]$ tal que $g(X) = (X - \alpha_2)h(X)$ e, assim,

$$f(X) = (X - \alpha_1)(X - \alpha_2)h(X).$$

□

O exemplo a seguir traz uma aplicação interessante do teste da raiz.

Exemplo 3.4 (União Soviética[1]). *Numere as linhas e colunas de um tabuleiro $n \times n$ de 1 a n, respectivamente de cima para baixo e da esquerda para a direita. Dados $2n$ números reais distintos $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, para $1 \leq i, j \leq n$ escreva o número $a_i + b_j$ na casa 1×1 situada na linha i e na coluna j. Se os produtos dos números escritos nas casas das colunas do tabuleiro forem todos iguais, prove que os produtos dos números escritos nas casas das linhas do mesmo também serão todos iguais.*

Prova. Considere o polinômio

$$f(X) = (X + a_1)(X + a_2)\ldots(X + a_n) \in \mathbb{R}[X].$$

Sendo $\tilde{f}$ a função polinomial associada a f, segue do enunciado a existência de $\alpha \in \mathbb{R}$ tal que $\tilde{f}(b_1) = \tilde{f}(b_2) = \cdots = \tilde{f}(b_n) = \alpha$. Então, $\tilde{f}(b_i) - \alpha = 0$ para $1 \leq i \leq n$, de modo que, pelo teste da raiz, temos

$$f(X) - \alpha = (X - b_1)(X - b_2)\ldots(X - b_n)$$

[1] A União Soviética foi um país que existiu até 1991, quando o colapso do Comunismo a fez dividir-se em vários países distintos, dentre os quais citamos Azerbaijão, Bielorrússia, Estônia, Cazaquistão, Letônia, Lutiânia, Moldávia, Rússia, Ucrânia e Uzbequistão.

(note que tanto $f(X) - \alpha$ quanto o polinômio do segundo membro na igualdade acima são mônicos e têm grau n). Portanto,

$$-\alpha = f(-a_i) - \alpha = (-1)^n(a_i + b_1)(a_i + b_2)\ldots(a_i + b_n),$$

de forma que os produtos dos números em cada linha são iguais a $(-1)^{n-1}\alpha$. □

Como corolário do teste da raiz, explicitamos a seguir um algoritmo bastante simples para a obtenção do quociente da divisão de um polinômio mônico $f \in \mathbb{K}[X]$ por $X - \alpha$, onde α é uma raiz de f. Tal algoritmo é conhecido na literatura como o **algoritmo de Horner-Ruffini**, e é baseado no resultado a seguir.

Proposição 3.5 (Horner-Ruffini). *Seja*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

um polinômio mônico sobre $\mathbb{K}$. Se $\alpha \in \mathbb{K}$ é uma raiz de f e

$$g(X) = X^{n-1} + b_{n-2}X^{n-2} + \cdots + b_0 \in \mathbb{K}[X]$$

é o quociente da divisão de $f(X)$ por $X - \alpha$, então

$$\left\{\begin{array}{lcl} b_{n-2} & = & \alpha + a_{n-1} \\ b_{n-3} & = & \alpha b_{n-2} + a_{n-2} \\ \cdots & & \cdots \\ b_{n-i-1} & = & \alpha b_{n-i} + a_{n-i} \\ \cdots & & \cdots \\ b_0 & = & \alpha b_1 + a_1 \end{array}\right. . \tag{3.1}$$

Prova. Por uniformidade de notação, faça $b_{n-1} = 1$. Temos inicial-

mente que

$$\begin{aligned}
f(X) &= (X-\alpha)g(X) = (X-\alpha)\sum_{i=0}^{n-1} b_{n-1-i}X^{n-1-i} \\
&= \sum_{i=0}^{n-1} b_{n-1-i}X^{n-i} - \sum_{i=0}^{n-1} \alpha b_{n-1-i}X^{n-1-i} \\
&= b_{n-1}X^n + \sum_{i=1}^{n-1} b_{n-1-i}X^{n-i} - \sum_{i=0}^{n-2} \alpha b_{n-1-i}X^{n-1-i} - \alpha b_0 \\
&= X^n + \sum_{i=1}^{n-1} b_{n-1-i}X^{n-i} - \sum_{i=1}^{n-1} \alpha b_{n-i}X^{n-i} - \alpha b_0 \\
&= X^n + \sum_{i=1}^{n-1} (b_{n-1-i} - \alpha b_{n-i})X^{n-i} - \alpha b_0.
\end{aligned}$$

Comparando a última expressão acima para f com aquela do enunciado, concluímos que

$$b_{n-1-i} - \alpha b_{n-i} = a_{n-i},$$

para $1 \leq i \leq n-1$. Obtemos, assim, o sistema de equações

$$\left\{\begin{array}{rcl}
b_{n-1} &=& 1 \\
b_{n-2} - \alpha b_{n-1} &=& a_{n-1} \\
b_{n-3} - \alpha b_{n-2} &=& a_{n-2} \\
\cdots && \cdots \\
b_{n-i-1} - \alpha b_{n-i} &=& a_{n-i} \\
\cdots && \cdots \\
b_0 - \alpha b_1 &=& a_1 \\
-\alpha b_0 &=& a_0.
\end{array}\right.,$$

o qual, por sua vez, equivale às relações do enunciado (a última equação do sistema acima pode ser desprezada, pois representa somente a condição de compatibilidade advinda da suposição de que α seja raiz de f). □

A discussão acima pode ser resumida na tabela a seguir, na qual colocamos os coeficientes de f (que não o coeficiente líder 1) na primeira linha e calculamos, da esquerda para a direita e a começar pelo coeficiente líder $b_{n-1} = 1$, os sucessivos coeficientes de g na segunda linha.

Algoritmo de Horner-Rufinni

a_{n-1}	a_{n-2}	a_{n-3}	$\cdots$	a_1	a_0
$b_{n-1} = 1$	$\underbrace{\alpha \cdot 1 + a_{n-1}}_{b_{n-2}}$	$\underbrace{\alpha \cdot b_{n-2} + a_{n-2}}_{b_{n-3}}$	$\cdots$	$\underbrace{\alpha \cdot b_2 + a_2}_{b_1}$	$\underbrace{\alpha \cdot b_1 + a_1}_{b_0}$

Observe que cada coeficiente de g, que não o líder, é igual ao produto do coeficiente à sua esquerda por α, somado ao coeficiente de f situado acima deste.

Exemplo 3.6. *Verifique que $\sqrt{2}$ é raiz do polinômio $f(X) = X^5 - 5X^4 + X^3 - 5X^2 - 6X + 30$ e encontre, com o auxílio do algoritmo de Horner-Rufinni, o quociente da divisão de f por $X - \sqrt{2}$.*

Solução. Montemos a tabela do algoritmo de Horner-Rufinni pondo $n = 5$ e $a_4 = -5$, $a_3 = 1$, $a_2 = -5$, $a_1 = -6$, $a_0 = 30$ na primeira linha. Começando com $b_4 = 1$ na primeira casa da segunda linha, obtemos sucessivamente $b_3 = \sqrt{2} \cdot 1 - 5$, $b_2 = \sqrt{2}b_3 + 1 = 3 - 5\sqrt{2}$, $b_1 = \sqrt{2}b_2 - 5 = -15 + 3\sqrt{2}$ e $b_0 = \sqrt{2}b_1 - 6 = -15\sqrt{2}$.

-5	1	-5	-6	30
1	$\sqrt{2} \cdot 1 - 5$	$3 - 5\sqrt{2}$	$-15 + 3\sqrt{2}$	$-15\sqrt{2}$

Por fim, como $-\alpha b_0 = -\sqrt{2}(-15\sqrt{2}) = 30 = a_0$, segue que $\sqrt{2}$ é realmente raiz de f e o quociente da divisão de f por $X - \sqrt{2}$ é $X^4 + (\sqrt{2} - 5)X^3 + (3 - 5\sqrt{2})X^2 + (-15 + 3\sqrt{2})X - 15\sqrt{2}$. □

Nas notações do teste da raiz, se $f(X) = (X - \alpha)^m q(X)$, com $\tilde{q}(\alpha) \neq 0$, dizemos que m é a **multiplicidade** de α como raiz de f. Em particular, α é uma raiz **simples** de f se $m = 1$ e **múltipla** se $m > 1$.

Exemplo 3.7. *Sendo* $f(X) = X^3 - 7X^2 + 16X - 12$ *um polinômio de coeficientes reais, temos que* 2 *é raiz dupla e* 3 *é raiz simples de* f*, uma vez que* $f(X) = (X - 2)^2(X - 3)$.

Mais adiante neste capítulo, estudaremos em detalhe o problema de examinar se um polinômio f com coeficientes em $\mathbb{K}$ possui ou não raízes múltiplas. Por ora, precisaremos no máximo saber o que vem a ser uma tal raiz. Devemos notar, todavia, que já temos uma maneira de saber se um elemento $\alpha \in \mathbb{K}$ é ou não raiz múltipla de um polinômio não nulo f: basta dividir f por $(X - \alpha)^2$ (o que pode ser feito com duas aplicações sucessivas do algoritmo de Horner-Rufinni) e verificar se a divisão é exata. Teremos mais a dizer sobre isso mais adiante.

Outro corolário interessante do algoritmo da divisão é o fato de um polinômio não identicamente nulo não poder ter mais raízes do que seu grau. Observe que permitimos raízes múltiplas no resultado a seguir.

Corolário 3.8. *Se* $f \in \mathbb{K}[X] \setminus \{0\}$*, então* f *possui no máximo* ∂f *raízes em* $\mathbb{K}$*, contadas de acordo com suas multiplicidades.*

Prova. Façamos indução sobre o grau de f. Se $\partial f = 0$, então existe $c \in \mathbb{K} \setminus \{0\}$ tal que $f(X) = c$. Daí, a função polinomial associada $\tilde{f}$ é a função constante $x \mapsto c$, e segue que o número de raízes de f é 0, igual a seu grau.

Seja, agora, f um polinômio de grau positivo e suponha a afirmação do enunciado válida para todos os polinômios não nulos de graus menores que ∂f. Se f não tiver raízes em $\mathbb{K}$, nada há a fazer. Senão, seja $\alpha \in \mathbb{K}$ uma raiz de f e (de acordo com o teste da raiz) m o

maior natural tal que $f(X) = (X - \alpha)^m q(X)$, para algum polinômio $q \in \mathbb{K}[X]$. Como

$$\partial q = \partial f - m < \partial f,$$

segue da hipótese de indução que q tem no máximo ∂q raízes em $\mathbb{K}$, contadas de acordo com suas multiplicidades. Agora, se $\beta \neq \alpha$ é raiz de f, temos

$$0 = \tilde{f}(\beta) = (\beta - \alpha)^m \tilde{q}(\beta)$$

e, daí, β é raiz de q. Portanto, o número de raízes de f é igual a m (a multiplicidade de α) mais o número de raízes de q, e segue, por hipótese de indução, que f possui no máximo

$$m + \partial q = \partial f$$

raízes em $\mathbb{K}$. □

Utilizamos frequentemente o corolário acima em uma das formas a seguir.

Corolário 3.9. *Se* $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{K}[X]$ *admite pelo menos* $n+1$ *raízes distintas em* $\mathbb{K}$*, então* f *é identicamente nulo, i.e.,* $a_n = \cdots = a_0 = 0$.

Prova. Se $f \in \mathbb{K}[X] \setminus \{0\}$, então, pelo corolário anterior, f teria no máximo n raízes em $\mathbb{K}$. □

Corolário 3.10. *Sejam* $f(X) = a_nX^n + \cdots + a_1X + a_0$ *e* $g(X) = b_mX^m + \cdots + b_1X + b_0$ *polinômios sobre* $\mathbb{K}$*, com* $m \geq n$*. Se* $\tilde{f}(x) = \tilde{g}(x)$ *para ao menos* $m+1$ *valores distintos* $x \in \mathbb{K}$*, então* $f = g$*, i.e,* $m = n$ *e* $a_i = b_i$*, para* $0 \leq i \leq n$.

Prova. Basta aplicar o corolário anterior ao polinômio $f - g$, notando que a função polinomial associada a tal polinômio é $\tilde{f} - \tilde{g}$. □

Se $\mathcal{F}$ é o conjunto das funções de $\mathbb{K}$ em $\mathbb{K}$, então o último corolário acima garante que a aplicação

$$\begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{F} \\ f & \longmapsto & \tilde{f} \end{array}, \tag{3.2}$$

que associa a cada polinômio $f \in \mathbb{K}[X]$ sua função polinomial $\tilde{f} \in \mathcal{F}$, é injetiva. Em outras palavras, ele afirma que dois polinômios sobre $\mathbb{K}$ só terão funções polinomiais iguais quando eles mesmos forem iguais[2].

Graças a esse fato, doravante vamos denotar por f tanto um elemento de $\mathbb{K}[X]$ (i.e., um polinômio com coeficientes em $\mathbb{K}$) quanto a função polinomial associada a tal elemento. Em particular, quando escrevermos $f(X)$, estaremos nos referindo ao *polinômio* f; quando escrevermos $f(x)$, estaremos nos referindo ao elemento de $\mathbb{K}$, imagem de $x \in \mathbb{K}$ pela função polinomial associada a f. O contexto esclarecerá eventuais confusões.

Observação 3.11. *O corolário 3.10 garante que os coeficientes de um polinômio $f \in \mathbb{K}[X]$ são determinados pelos valores $f(x)$, com $x \in \mathbb{K}$. Posteriormente, estudaremos em detalhe o problema de como obter um polinômio em $\mathbb{K}[X]$ que assuma valores prescritos em um número finito de elementos $x \in \mathbb{K}$ dados.*

Os dois exemplos a seguir ilustram usos típicos dos corolários 3.9 e 3.10.

Exemplo 3.12 (Moldávia). *Obtenha todos os polinômios $f \in \mathbb{R}[X]$ tais que $f(0) = 0$ e*

$$f(x^2 + 1) = f(x)^2 + 1, \ \forall x \in \mathbb{R}.$$

[2]Conforme veremos na seção 7.3, ao desenvolvermos a teoria de polinômios sobre $\mathbb{Z}_p$, onde $p \in \mathbb{Z}$ é primo, o fato de $\mathbb{K}$ ser infinito nos casos presentemente sob consideração é imprescindível para a injetividade de (3.2).

Solução. Defina a sequência $(u_n)_{n\geq 0}$ por $u_0 = 0$ e $u_{n+1} = u_n^2 + 1$, para $n \geq 1$. Se $g(X) = X$, então $f(u_0) = 0 = g(u_0)$ e, supondo $f(u_k) = g(u_k)$, temos também

$$\begin{aligned} f(u_{k+1}) &= f(u_k^2 + 1) = f(u_k)^2 + 1 \\ &= g(u_k)^2 + 1 = u_k^2 + 1 \\ &= g(u_{k+1}). \end{aligned}$$

Portanto, por indução temos $f(u_n) = g(u_n)$, para todo inteiro não negativo n. Mas, como os valores dos termos u_n são dois a dois distintos, concluímos que f e g coincidem em uma quantidade infinita de valores distintos, e segue do corolário 3.10 que $f = g$, i.e., $f(X) = X$. □

Exemplo 3.13 (Hong Kong). *Seja $g(X) = X^5 + X^4 + X^3 + X^2 + X + 1$. Calcule resto da divisão de $g(X^{12})$ por $g(X)$.*

Solução. Pelo algoritmo da divisão, existe $q, r \in \mathbb{R}[X]$ tais que

$$g(X^{12}) = g(X)q(X) + r(X),$$

com $r = 0$ ou $0 \leq \partial r \leq 4$. Tomando $\omega = \text{cis}\,\frac{2\pi}{6}$ e fazendo $x = \omega^k$ nas funções polinomiais correspondentes, com $1 \leq k \leq 5$, obtemos

$$g(\omega^{12k}) = g(\omega^k)q(\omega^k) + r(\omega^k), \tag{3.3}$$

para $1 \leq k \leq 5$.

Agora, como $\omega^{12k} = \text{cis}\,(4k\pi) = 1$, temos $g(\omega^{12k}) = g(1) = 6$. Por outro lado, para $1 \leq k \leq 5$, o lema 1.12 fornece

$$g(\omega^k) = \omega^{5k} + \omega^{4k} + \omega^{3k} + \omega^{2k} + \omega^k + 1 = \frac{\omega^{6k} - 1}{\omega^k - 1} = 0.$$

Assim, (3.3) se reduz a $r(\omega^k) = 6$, para $1 \leq k \leq 5$, de sorte que o polinômio $r - 6$ tem pelo menos cinco raízes distintas. Mas, como $r - 6 = 0$ ou $\partial(r - 6) \leq 4$, segue do corolário 3.8 que $r - 6 = 0$. □

O corolário a seguir garante que a imagem da função polinomial associada a um polinômio não constante é um conjunto infinito.

Corolário 3.14. *Se $f \in \mathbb{K}[X] \setminus \mathbb{K}$, então a imagem* $\text{Im}(f)$ *da função polinomial associada a f é um subconjunto infinito de $\mathbb{K}$.*

Prova. Suponha o contrário, i.e, que $\text{Im}(f) = \{\alpha_1, \ldots, \alpha_k\} \subset \mathbb{K}$. Então, para todo $x \in \mathbb{K}$, teríamos $f(x) \in \{\alpha_1, \ldots, \alpha_k\}$. Mas, como $\mathbb{K}$ é um conjunto infinito, existiriam $1 \leq i \leq k$ e elementos dois a dois distintos $x_1, x_2, \ldots \in \mathbb{K}$ tais que

$$f(x_1) = f(x_2) = \cdots = \alpha_i.$$

Portanto, $f(X) - \alpha_i$ seria um polinômio não identicamente nulo (lembre-se de que f é não constante) com uma infinidade de raízes distintas, o que é uma contradição. $\square$

Exemplo 3.15 (Canadá). *Ache todos os polinômios não constantes $f \in \mathbb{Q}[X]$ que satisfazem a relação $f(f(X)) = f(X)^k$, onde k é um inteiro positivo dado.*

Solução. É fácil ver (conforme problema 1) que, para todo $x \in \mathbb{Q}$, temos $f(f(x)) = f(x)^k$. De outro modo, $f(y) = y^k$, para todo $y \in \text{Im}(f)$. Mas, o corolário 3.14 garante que $\text{Im}(f)$ é um subconjunto infinito de $\mathbb{Q}$, de sorte que o corolário 3.10 garante que $f(X) = X^k$. $\square$

Terminamos esta seção estudando o problema de pesquisa de raízes racionais de polinômios de coeficientes inteiros. O item (a) da proposição a seguir traz o resultado central, conhecido na literatura como o **critério de pesquisa de raízes racionais** de polinômios de coeficientes inteiros.

Proposição 3.16. *Sejam $n > 1$ inteiro, $f(X) = a_nX^n + \cdots + a_1X + a_0$ um polinômio de coeficientes inteiros e p e q inteiros não nulos primos entre si. Se $f(\frac{p}{q}) = 0$, então:*

(a) $p \mid a_0$ e $q \mid a_n$.

(b) Se f for mônico, as possíveis raízes racionais de f são inteiras.

(c) $(p - mq) \mid f(m)$, para todo $m \in \mathbb{Z}$. Em particular, $(p - q) \mid f(1)$ e $(p + q) \mid f(-1)$.

Prova.
(a) A partir de $f(\frac{p}{q}) = 0$, obtemos prontamente

$$a_np^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^{n-1} + a_0q^n = 0$$

e, daí,

$$\begin{cases} a_0q^n &= p(-a_np^{n-1} - \cdots - a_1q^{n-1}) \\ a_np^n &= q(-a_{n-1}p^{n-1} - \cdots - a_0q^{n-1}) \end{cases}.$$

Portanto, $p \mid a_0q^n$ e $q \mid a_np^n$. Mas, uma vez que p e q são primos entre si, o item (a) da proposição 1.21 de [14] garante que $p \mid a_0$ e $q \mid a_n$, como queríamos provar.

(b) Imediato a partir de (a).

(c) Como $f(\frac{p}{q}) = 0$, temos $f(m) = f(m) - f(\frac{p}{q})$ ou, ainda,

$$f(m) = (a_nm^n + \cdots + a_1m + a_0) - \frac{1}{q^n}(a_np^n + \cdots + a_1pq^{n-1} + a_0q^n).$$

Portanto,

$$\begin{aligned} q^nf(m) &= q^n(a_nm^n + \cdots + a_1m + a_0) - (a_np^n + \cdots + a_1pq^{n-1} + a_0q^n) \\ &= a_n((mq)^n - p^n) + \cdots + a_1q^{n-1}(mq - p) = (mq - p)r, \end{aligned}$$

para algum $r \in \mathbb{Z}$, onde utilizamos o item (a) do problema 2.1.18 de [10] na última igualdade acima. Os cálculos acima garantem que $(mq - p) \mid q^nf(m)$. A partir daí, para concluir que $(mq - p) \mid f(m)$,

é suficiente, novamente pelo item (a) da proposição 1.21 de [14], mostrarmos que $\text{mdc}\,(mq-p,q^n)=1$. Para tanto, basta aplicarmos o item (b) da proposição 1.21 e o corolário 1.22 de [14] para obter

$$\text{mdc}\,(p,q)=1 \Rightarrow \text{mdc}\,(mq-p,q)=1 \Rightarrow \text{mdc}\,(mq-p,q^n)=1.$$

O resto é imediato. □

A proposição anterior pode, por vezes, ser aplicada para garantir a irracionalidade de números reais. Vejamos alguns exemplos.

Exemplo 3.17. *Prove que o número* $\sqrt{2+\sqrt{2+\sqrt{2}}}$ *é irracional.*

Prova. Se $\alpha=\sqrt{2+\sqrt{2+\sqrt{2}}}$, então $\alpha^2-2=\sqrt{2+\sqrt{2}}$ e, daí, $(\alpha^2-2)^2=2+\sqrt{2}$. Logo, $((\alpha^2-2)^2-2)^2=2$, de maneira que α é raiz do polinômio mônico de coeficientes inteiros

$$\begin{aligned} f(X) &= ((X^2-2)^2-2)^2-2 \\ &= (X^4-4X^2+2)^2-2. \end{aligned}$$

Portanto, se $\alpha\in\mathbb{Q}$, segue dos itens (a) e (b) da proposição anterior que $\alpha\in\mathbb{N}$ e $\alpha\mid f(0)=2$, de modo que $\alpha=1$ ou 2. Mas, como

$$1<\alpha<\sqrt{2+\sqrt{2+2}}=2,$$

chegamos a uma contradição. □

Exemplo 3.18. *Prove que* $\text{tg}\,10^\circ$ *é irracional.*

Prova. Denotemos $\alpha=\text{tg}\,10^\circ$. Aplicando a proposição 7.18 e o corolário 7.19 de [11], obtemos sucessivamente

$$\begin{aligned} \text{tg}\,30^\circ &= \frac{\text{tg}\,20^\circ+\text{tg}\,10^\circ}{1-\text{tg}\,20^\circ\cdot\text{tg}\,10^\circ}=\frac{\frac{2\,\text{tg}\,10^\circ}{1-\text{tg}^2 10^\circ}+\text{tg}\,10^\circ}{1-\frac{2\,\text{tg}^2 10^\circ}{1-\text{tg}^2 10^\circ}} \\ &= \frac{\frac{2\alpha}{1-\alpha^2}+\alpha}{1-\frac{2\alpha^2}{1-\alpha^2}}=\frac{3\alpha-\alpha^3}{1-3\alpha^2} \end{aligned}$$

Mas, como $\text{tg}\,30^\circ=\frac{1}{\sqrt{3}}$, segue que

$$\frac{(3\alpha-\alpha^3)^2}{(1-3\alpha^2)^2}=\frac{1}{3}$$

ou, ainda,

$$3\alpha^6-27\alpha^4+33\alpha^2-1=0.$$

Portanto, $\text{tg}\,10^\circ$ é raiz do polinômio de coeficientes inteiros $f(X)=3X^6-27X^4+33X^2-1$, e basta mostrar que o mesmo não possui raízes racionais. Para tanto, note inicialmente que, pela proposição 3.16, as possíveis raízes racionais de f são ±1 ou $\pm\frac{1}{3}$; entretanto, calculando diretamente $f(\pm1)$ e $f(\pm\frac{1}{3})$ concluímos que nenhum desses números é igual a 0, conforme desejado. □

Exemplo 3.19 (Iugoslávia[3]). *Ache todos os racionais positivos* $a\leq b\leq c$ *tais que os números*

$$a+b+c,\ \frac{1}{a}+\frac{1}{b}+\frac{1}{c}\ \text{e}\ abc$$

sejam todos inteiros.

Solução. Se $f(X)=(X-a)(X-b)(X-c)$, então a,b e c são as raízes de f, ademais racionais. Por outro lado,

$$f(X)=X^3-(a+b+c)X^2+(ab+bc+ca)X-abc,$$

com

$$ab+bc+ca=abc\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)\in\mathbb{Z}.$$

Segue, então, que $f\in\mathbb{Z}[X]$. Mas, como f é mônico, o critério de pesquisa de raízes racionais aplicado a f garante que a,b e c são inteiros. Por fim, uma vez que a, b e c são positivos, as condições do enunciado

[3]Até a década de 1990, Bósnia e Herzegovina, Croácia, Eslovênia, Kosovo, Macedônia, Montenegro e Sérvia compunham um único país, a Iugoslávia.

garantem que basta encontrarmos todos os $a \leq b \leq c$ naturais para os quais $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}$ também seja natural. Este é um problema simples, o qual será deixado ao leitor; as únicas soluções são os ternos

$$(a, b, c) = (1, 1, 1), (1, 2, 2), (3, 3, 3), (2, 4, 4) \text{ ou } (2, 3, 6).$$

□

Problemas – Seção 3.1

1. * Mostre que a definição usual de função composta de duas funções de $\mathbb{K}$ em $\mathbb{K}$, quando aplicada a polinômios $f, g \in \mathbb{K}[X]$ de graus respectivamente m e n, produz um polinômio em $\mathbb{K}[X]$, de grau mn. Denotando tal polinômio também por $f \circ g$, mostre ainda que a função polinomial associada ao mesmo coincide com a função composta $\tilde{f} \circ \tilde{g}$, onde $\tilde{f}$ e $\tilde{g}$ denotam, respectivamente, as funções polinomiais associadas a f e g.

2. * Sejam a, b e r números racionais, onde $r > 0$ é tal que $\sqrt{r}$ é irracional. Faça os seguintes itens:

   (a) Para $k \in \mathbb{N}$ fixado, mostre que existem $a_k, b_k \in \mathbb{Q}$ tais que $(a \pm b\sqrt{r})^k = a_k \pm b_k\sqrt{r}$.

   (b) Se $f \in \mathbb{Q}[X] \setminus \{0\}$, prove que $f(a + b\sqrt{r}) = 0 \Leftrightarrow f(a - b\sqrt{r}) = 0$.

3. Uma das raízes do polinômio $X^4 + aX^3 + X^2 + bX - 2$ é $1 - \sqrt{2}$. Encontre as demais raízes, sabendo que a e b são ambos racionais.

4. Sejam dados $a, b \in \mathbb{K}$, sendo $a \neq 0$. Para $f \in \mathbb{K}[X] \setminus \{0\}$, prove que o resto da divisão de f por $aX + b$ é igual a $f\left(-\frac{b}{a}\right)$.

5. Existe um polinômio $f \in \mathbb{R}[X]$, tal que $f(\operatorname{sen} x) = \cos x$ para todo real x? Justifique sua resposta.

6. Seja $\alpha \neq k\pi$ um número complexo. Prove que o polinômio X^2+1 divide o polinômio

$$f(X) = (\cos\alpha + X\operatorname{sen}\alpha)^n - \cos(n\alpha) - \operatorname{sen}(n\alpha)X.$$

7. (Canadá.) Seja f um polinômio não nulo e de coeficientes inteiros. Se $f(0)$ e $f(1)$ são ímpares, prove que f não possui raízes inteiras.

8. (Canadá.) Prove que não existem x, y e z inteiros não nulos em PA, tais que $x^5 + y^5 = z^5$.

9. Mostre que, dado $n \in \mathbb{N}$, existe um único polinômio[4] f_n tal que

$$f_n(2\cos\theta) = 2\cos(n\theta),$$

   para todo $\theta \in \mathbb{R}$. Mostre ainda que:

   (a) $f_1(X) = X$, $f_2(X) = X^2 - 1$ e, para $k \geq 1$ inteiro,

$$f_{k+2}(X) = Xf_{k+1}(X) - f_k(X).$$

   (b) f_n é mônico, de coeficientes inteiros e grau n.

   (c) $f_n\left(z + \frac{1}{z}\right) = z^n + \frac{1}{z^n}$, para todo $z \in \mathbb{C} \setminus \{0\}$.

10. Encontre todos os $\alpha \in \mathbb{Q}$ para os quais $\cos(\alpha\pi) \in \mathbb{Q}$.

11. (BMO.) Para $m \in \mathbb{Z}$, prove que o polinômio

$$X^4 - 1994X^3 + (1993 + m)X^2 - 11X + m$$

   não possui duas raízes inteiras distintas.

[4]Os polinômios f_n de que trata este problema são conhecidos na literatura como os **polinômios de Chebyshev**, em homenagem ao matemático russo do século XIX Pafnuty L. Chebyshev.

12. (AIME.) Encontre todos os reais a e b tais que $X^2 - X - 1$ divide $aX^{17} + bX^{16} + 1$.

13. (Moldávia.) Seja $n > 4$ um natural dado e p um polinômio mônico, de grau n e com n raízes inteiras distintas, uma das quais igual a 0. Calcule o número de raízes inteiras e distintas do polinômio $p(p(X))$.

14. (Áustria-Polônia.) Seja $f(x) = ax^3 + bx^2 + cx + d$ um polinômio de coeficientes inteiros e grau 3. Prove que não é possível achar quatro primos distintos p_1, p_2, p_3 e p_4 para os quais

$$|f(p_1)| = |f(p_2)| = |f(p_3)| = |f(p_4)| = 3.$$

15. (Canadá.) Seja $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ um polinômio de coeficientes inteiros, e suponha que existam inteiros distintos a, b, c e d tais que $p(a) = p(b) = p(c) = p(d) = 5$. Prove que não existe inteiro m tal que $p(m) = 8$.

16. Ache todos os valores $k \in \mathbb{N}$ tais que o polinômio $X^2 + X + 1$ divide o polinômio $X^{2k} + 1 + (X + 1)^{2k}$.

Para o exemplo a seguir, lembre-se (cf. parágrafo anterior ao problema 1.4.11 de [13]) de que um *multiconjunto* é uma coleção $\{\{a_1, a_2, \ldots, a_n\}\}$ de elementos não necessariamente distintos, com $\{\{a_1, a_2, \ldots, a_n\}\} = \{\{b_1, b_2, \ldots, b_m\}\}$ se $m = n$ e cada elemento aparecer uma mesma quantidade de vezes em cada um deles.

17. Sejam $\{\{a_1, a_2, \ldots, a_n\}\}$ e $\{\{b_1, b_2, \ldots, b_n\}\}$ dois multiconjuntos distintos, cada um dos quais formado por inteiros positivos. Se

$$\{\{a_i + a_j;\ 1 \leq i < j \leq n\}\} = \{\{b_i + b_j;\ 1 \leq i < j \leq n\}\},$$

prove que n é uma potência de 2.

3.2 Raízes da unidade e contagem

Nesta curta seção, paramos momentaneamente a apresentação da teoria geral de polinômios para ilustrar o papel das raízes da unidade como ferramenta de contagem. Uma vez que a aplicabilidade de argumentos algébricos em Combinatória é muitíssimo mais ampla do que conseguiremos mostrar aqui, recomendamos ao leitor a excelente referência [55] para uma abordagem abrangente.

Comecemos examinando, no exemplo a seguir, como utilizar números complexos como *marcadores*.

Exemplo 3.20. *Em um círculo há $n > 1$ lâmpadas igualmente espaçadas. Inicialmente, exatamente uma delas está acesa. Uma operação permitida sobre o estado das lâmpadas é escolher um divisor positivo d de n, tal que $d < n$, e mudar o estado de $\frac{n}{d}$ lâmpadas igualmente espaçadas, contanto que o estado inicial de todas elas seja o mesmo. Existe uma sequência de operações que deixe todas as n lâmpadas acesas?*

Prova. Não. Por contradição, suponha, sem perda de generalidade, que o círculo é o círculo unitário do plano complexo e que as lâmpadas estão posicionadas nos pontos $1, \omega, \ldots, \omega^{n-1}$, onde $\omega = \text{cis}\,\frac{2\pi}{n}$. Suponha ainda (também sem perda de generalidade) que a lâmpada inicialmente acesa está posicionada em 1.

Para $k \geq 0$, seja a_k a soma dos números complexos associados às lâmpadas acesas imediatamente antes da $(k+1)-$ésima operação, de sorte que $a_0 = 1$. Na $(k+1)-$ésima operação, escolhemos lâmpadas posicionadas em

$$\omega^l,\ \omega^{l+d},\ \omega^{l+2d},\ \ldots,\ \omega^{l+(\frac{n}{d}-1)d},$$

para algum par (l, d) de inteiros tais que $0 \leq l < d$ e $d \mid n$, com $d < n$.

Mas, uma vez que $\omega^n = 1$, temos

$$\begin{aligned} a_{k+1} &= a_k \pm (\omega^l + \omega^{l+d} + \omega^{l+2d} + \cdots + \omega^{l+(\frac{n}{d}-1)d}) \\ &= a_k \pm \frac{\omega^{l+(\frac{n}{d}-1)d} \cdot \omega^d - \omega^l}{\omega^d - 1} = a_k, \end{aligned}$$

e segue que $a_k = 1$, para todo $k \geq 0$.

Por fim, se após m operações todas as lâmpadas resultassem acesas, teríamos

$$a_m = 1 + \omega + \cdots + \omega^n = 0,$$

o que é uma contradição. □

Agora, dados $m, n, p \in \mathbb{N}$, consideremos a tarefa de construir um retângulo $m \times n$ utilizando peças $1 \times p$. Contando quadradinhos 1×1, obtemos uma condição necessária óbvia para que a construção proposta seja possível: p deve dividir mn. Por outro lado, é claro que, se p dividir m ou n, então tal construção é sempre possível: sendo, por exemplo, $m = pk$, com $k \in \mathbb{N}$, podemos montar nosso retângulo $m \times n$ justapondo k retângulos $p \times n$, cada um dos quais construído empilhando n peças $1 \times p$. O fato interessante é que a recíproca da discussão acima é verdadeira, i.e., só será possível montar nosso retângulo se p dividir m ou n. Esse é o conteúdo do teorema a seguir, devido ao matemático americano David Klarner[5].

Teorema 3.21 (Klarner). *Sejam m, n, p naturais dados. Se pudermos cobrir um tabuleiro $m \times n$ usando peças $1 \times p$, sem sobras ou superposições de peças, então p deve dividir m ou n.*

Prova. Suponha que possamos cobrir o tabuleiro como se pede e notemos inicialmente que $p \leq \max\{m, n\}$. Particione o tabuleiro em m linhas $1 \times n$ e n colunas $1 \times m$, numerando as linhas de cima para baixo, de 1 a m, e as colunas da esquerda para a direita, de 1 a n (como em

[5]Cf. [36]. Contudo, a demonstração apresentada difere da original.

uma matriz $m \times n$). Em seguida, escreva, na casa do tabuleiro situada à linha i e coluna j, o número complexo ω^{i+j}, onde $\omega = \text{cis}\,\frac{2\pi}{p}$.

Calculemos, agora, a soma dos números escritos nas casas do tabuleiro de duas maneiras distintas (eis aqui uma contagem dupla!). Por um lado, tal soma é claramente igual a

$$(\omega + \omega^2 + \cdots + \omega^n)(\omega + \omega^2 + \cdots + \omega^m) = \frac{\omega^2(\omega^n - 1)(\omega^m - 1)}{(\omega - 1)^2}, \quad (3.4)$$

onde utilizamos o lema 1.12 na igualdade acima; por outro, como estamos supondo ser possível cobrir o tabuleiro como pedido, os números escritos no mesmo podem ser agrupados em conjuntos de p números, correspondentes às p casas horizontais ou verticais cobertas por cada peça $1 \times p$ utilizada. Tais conjuntos de p números dão origem a somas de um dos tipos

$$\omega^{i+j} + \omega^{i+(j+1)} + \cdots + \omega^{i+(j+p-1)}$$

ou

$$\omega^{i+j} + \omega^{(i+1)+j} + \cdots + \omega^{(i+p-1)+j},$$

conforme a peça $1 \times p$ seja respectivamente horizontal ou vertical. Novamente pelo lema 1.12 e pela primeira fórmula de de Moivre, cada uma de tais somas é igual

$$\omega^{i+j}(1 + \omega + \cdots + \omega^{p-1}) = \omega^{i+j} \cdot \frac{\omega^p - 1}{\omega - 1} = 0$$

e, portanto, a soma de todos os números escritos no tabuleiro deve também ser igual a 0. Então, segue de (3.4) que $(\omega^n - 1)(\omega^m - 1) = 0$ ou, ainda, que

$$\text{cis}\,\frac{2n\pi}{p} = 1 \quad \text{ou} \quad \text{cis}\,\frac{2m\pi}{p} = 1.$$

Por fim, é imediato, a partir de tais igualdades, que p divide n ou m. □

O teorema a seguir traz uma ferramenta algébrica bastante útil em várias situações combinatórias, sendo conhecida como a **fórmula de multiseção**.

Teorema 3.22. *Para $f \in \mathbb{C}[X] \setminus \{0\}$, denote por a_k o coeficiente de X^k em f. Se p é um número primo e $\omega \neq 1$ é uma raiz $p-$ésima da unidade, então*

$$\sum_{p|k} a_k = \frac{1}{p}(f(1) + f(\omega) + \cdots + f(\omega^{p-1})). \tag{3.5}$$

Prova. Como $f(X) = \sum_{j\geq 0} a_j X^j$, temos

$$\begin{aligned} \sum_{k=0}^{p-1} f(\omega^k) &= \sum_{k=0}^{p-1}\sum_{j\geq 0} a_j\omega^{jk} = \sum_{j\geq 0}\sum_{k=0}^{p-1} a_j\omega^{jk} \\ &= \sum_{j\geq 0} a_j \sum_{k=0}^{p-1}\omega^{jk}. \end{aligned} \tag{3.6}$$

Note agora que, se $p \mid j$, então $\omega^{jk} = 1$ para todo k, de sorte que $\sum_{k=0}^{p-1}\omega^{jk} = p$. Por outro lado, se $p \nmid j$, então o item (a) da proposição 6.3 de [14] garante que $\{0, j, 2j, \ldots, (p-1)j\}$ é um SCR[6] módulo p. Portanto, ainda nesse caso, temos

$$\sum_{k=0}^{p-1}\omega^{jk} = \sum_{k=0}^{p-1}\omega^{k} = \frac{\omega^p - 1}{\omega - 1} = 0,$$

e (3.6) fornece

$$\begin{aligned} \sum_{k=0}^{p-1} f(\omega^k) &= \sum_{j\geq 0} a_j \sum_{k=0}^{p-1}\omega^{jk} = \sum_{l\geq 0} a_{pl}]p \\ &= p\sum_{l\geq 0} a_{pl} = p\sum_{p|k} a_k. \end{aligned}$$

[6]Recorde que um *sistema completo de restos* (abreviado *SCR*) módulo p é um conjunto $\{a_0, a_1, \ldots, a_{p-1}\}$ de números inteiros tais que, a menos de uma permutação, tenhamos $a_j \equiv j \pmod{p}$, para $0 \leq j \leq p-1$.

□

Exemplo 3.23 (Polônia). *Para cada inteiro positivo n, calcule, em função de n, o valor da soma*

$$\sum_{3|k}\binom{n}{k}.$$

Solução. Seja

$$f(X) = (X+1)^n = \sum_{k=0}^{n}\binom{n}{k}X^k.$$

Sendo $\omega = \operatorname{cis}\frac{2\pi}{3}$, raiz cúbica da unidade, temos $1 + \omega + \omega^2 = 0$ e segue, da fórmula de multiseção aplicada a f, que

$$\begin{aligned} \sum_{3|k}\binom{n}{k} &= \frac{1}{3}\left(f(1) + f(\omega) + f(\omega^2)\right) \\ &= \frac{1}{3}\left(2^n + (\omega+1)^n + (\omega^2+1)^n\right) \\ &= \frac{1}{3}\left(2^n + (-\omega^2)^n + (-\omega)^n\right) \\ &= \frac{1}{3}\left(2^n + (-1)^n(\omega^{2n} + \omega^n)\right). \end{aligned}$$

Note agora que, se $3 \mid n$, então $\omega^n = 1$ e, daí, $\omega^{2n} + \omega^n = 2$; se $3 \nmid n$, então $\omega^n = \omega$ ou ω^2, de sorte que $\omega^{2n} + \omega^n = \omega^2 + \omega = -1$. Portanto,

$$\sum_{3|k}\binom{n}{k} = \begin{cases} (2^n + 2(-1)^n)/3, & \text{se } 3 \mid n \\ (2^n + (-1)^{n+1})/3, & \text{se } 3 \nmid n \end{cases}.$$

□

Problemas – Seção 3.2

1. Prove a seguinte extensão do teorema de Klarner: dados números naturais m, n, p e q tais que $1 < q \leq \min\{m, n, p\}$, podemos particionar um tabuleiro $m \times n \times p$ usando peças $1 \times q$ se, e só se, q dividir m, n ou p.

2. Podemos generalizar ainda mais o teorema de Klarner como segue (veja [36]): dados $m_1, \ldots, m_n \in \mathbb{N}$, seja
$$A = I_{m_1} \times \cdots \times I_{m_n},$$
o conjunto das sequências $(x_1, \ldots, x_n)$ de inteiros positivos tais que $1 \leq x_k \leq m_k$, para $1 \leq k \leq n$. Um *bloco de dimensões* $(1, \ldots, 1, p)$ *em* A é um subconjunto de A formado por p sequências $(x_{11}, \ldots, x_{1n})$, $\ldots$, $(x_{p1}, \ldots, x_{pn})$ satisfazendo a seguinte condição: existe $1 \leq k \leq n$ tal que:

   (a) $x_{1j} = x_{2j} = \cdots = x_{pj}$, para todo $1 \leq j \leq n$, $j \neq k$.

   (b) $(x_{1k}, x_{2k}, \ldots, x_{pk})$ é uma sequência de p inteiros consecutivos.

   Dizemos que o conjunto A pode ser *particionado em blocos de tamanho* $(1, \ldots, 1, p)$ se A puder ser escrito como a união disjunta de blocos desse tipo. Prove que tal é possível se, e só se, p dividir um dos números $m_1, \ldots, m_n$.

3. (Rússia.) Desejamos particionar o conjunto dos naturais de quatro algarismos em conjuntos de quatro números cada, de modo que a seguinte propriedade seja satisfeita: os quatro números de cada conjunto têm os mesmos algarismos em três posições e, na posição restante, seus algarismos são consecutivos (por exemplo, uma possibilidade para os quatro números de um conjunto poderia ser 1265, 1275, 1285 e 1295). Prove que não existe uma tal partição.

4. Seja n um natural dado e, para $0 \leq k \leq 2n$, seja a_k o coeficiente de X^k na expansão de $f(X) = (1 + X + X^2)^n$. Calcule, em função de n, o valor da soma
$$a_3 + a_6 + a_9 + \cdots.$$

5. * Generalize a fórmula de multiseção do seguinte modo: dados $f \in \mathbb{C}[X] \setminus \{0\}$, p primo ímpar e $0 \leq r \leq p-1$ inteiro, se $\omega \neq 1$ é uma raiz $p-$ésima da unidade, então
$$\sum_{k \equiv r \pmod p} a_k = \frac{1}{p} \sum_{j=0}^{p-1} \omega^{(p-1)rj} f(\omega^j),$$
onde a_k denota o coeficiente de X^k em f.

6. Calcule, em função de n, o valor da soma
$$\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \binom{n}{10} + \cdots.$$

3.3 O teorema fundamental da álgebra

Como caso particular do corolário 3.9, todo polinômio de coeficientes complexos e grau n possui no máximo n raízes complexas. Por outro lado, o polinômio $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ tem coeficientes racionais mas não admite raízes racionais; da mesma forma, o polinômio $g(X) = X^2 + 1 \in \mathbb{R}[X]$ tem coeficientes reais mas não admite raízes reais. Em ambos os casos, o fato de tais polinômios não admitirem raízes em $\mathbb{Q}$ ou $\mathbb{R}$ se deve a *deficiências* de tais conjuntos numéricos, no sentido de que, neles, não é possível realizarmos certas extrações de raízes.

Em sua tese de doutoramento, em 1799, o matemático alemão Carl F. Gauss mostrou, contrariamente aos casos examinados acima, que

todo polinômio sobre $\mathbb{C}$ admite raízes também em $\mathbb{C}$. Esse é o conteúdo do teorema a seguir, conhecido na literatura como o **teorema fundamental da álgebra**. A demonstração que apresentamos é devida a Jean-Baptiste le Rond d'Alembert, matemático francês do século XVIII.

Teorema 3.24 (Gauss). *Todo polinômio $f \in \mathbb{C}[X] \setminus \mathbb{C}$ possui ao menos uma raiz complexa.*

Prova. Por comodidade de notação, escrevamos $f(z) = a_n z^n + \cdots + a_1 z + a_0$ para denotar a função polinomial associada a f; sem perda de generalidade, podemos supor $a_0 \neq 0$.

Para $z \neq 0$, a desigualdade triangular para números complexos nos dá

$$\begin{aligned} |f(z)| &= |z|^n \left| a_n + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_0}{z^n} \right| \\ &\geq |z|^n \left(|a_n| - \frac{|a_{n-1}|}{|z|} - \frac{|a_{n-2}|}{|z|^2} - \cdots - \frac{|a_0|}{|z|^n} \right). \end{aligned}$$

Portanto, para

$$|z| > \max \left\{ \frac{2n|a_{n-1}|}{|a_n|}, \frac{\sqrt{2n|a_{n-2}|}}{\sqrt{|a_n|}}, \ldots, \frac{\sqrt[n]{2n|a_0|}}{\sqrt[n]{|a_n|}} \right\}, \tag{3.7}$$

temos $\frac{|a_{n-k}|}{|z|^k} < \frac{|a_n|}{2n}$, de sorte que

$$|f(z)| > |z|^n \left(|a_n| - n\frac{|a_n|}{2n} \right) = \frac{|a_n|}{2}|z|^n.$$

Mas, como $|z| > \sqrt[n]{\frac{2n|a_0|}{|a_n|}}$, temos $|a_n||z|^n > 2n|a_0|$ e, daí, $|f(z)| > n|a_0| \geq |a_0|$.

Em resumo, denotando por R o segundo membro de (3.7), concluímos que

$$|z| > R \Rightarrow |f(z)| > |a_0| = |f(0)|.$$

Agora, na seção 9.2 mostraremos (veja o corolário 9.20) que existe $z_0 \in \mathbb{C}$ tal que $|z_0| \leq R$ e

$$|f(z_0)| = \min\{|f(z)|;\ z \in \mathbb{C},\ |z| \leq R\}.$$

Portanto, segue do que fizemos acima que

$$|f(z_0)| = \min\{|f(z)|;\ z \in \mathbb{C}\}.$$

Por contradição, suponha que $f(z_0) \neq 0$ e mostremos que existe $h \in \mathbb{C}$ tal que $|f(z_0+h)| < |f(z_0)|$. Para tanto, comecemos observando que é imediato que existem $c_0, c_1, \ldots, c_n \in \mathbb{C}$, independentes de h e tais que

$$\begin{aligned} f(z_0 + h) &= a_0 + a_1(z_0 + h) + \cdots + a_n(z_0 + h)^n \\ &= c_0 + c_1 h + \cdots + c_n h^n; \end{aligned}$$

ademais, $c_0 = f(z_0) \neq 0$ e $c_n = a_n \neq 0$. Tome o menor $1 \leq k \leq n$, tal que $c_k \neq 0$. Então, fazendo $d_j = \frac{c_j}{c_0}$ para $0 \leq j \leq n$, temos

$$\begin{aligned} \frac{|f(z_0 + h)|}{|f(z_0)|} &= |1 + d_k h^k + d_{k+1} h^{k+1} + \cdots + d_n h^n| \\ &\leq |1 + d_k h^k| + |d_{k+1} h^{k+1} + \cdots + d_n h^n| \\ &= |1 + d_k h^k| + |d_k h^k| \left| \frac{d_{k+1}}{d_k} h + \cdots + \frac{d_n}{d_k} h^{n-k} \right|. \end{aligned}$$

Agora, estimativas análogas às que fizemos com o auxílio de (3.7), nos permitem escolher $r > 0$ tal que $|h| \leq r \Rightarrow \left| \frac{d_{k+1}}{d_k} h + \cdots + \frac{d_n}{d_k} h^{n-k} \right| < \frac{1}{2}$. Então,

$$|h| \leq r \Rightarrow \frac{|f(z_0 + h)|}{|f(z_0)|} \leq |1 + d_k h^k| + \frac{1}{2}|d_k h^k|.$$

Seja $d_k = s \operatorname{cis} \alpha$ e faça $h = r \operatorname{cis} \theta$. A primeira fórmula de de Moivre nos dá

$$\frac{|f(z_0 + h)|}{|f(z_0)|} \leq |1 + sr^k \operatorname{cis}(\alpha + k\theta)| + \frac{1}{2} sr^k;$$

portanto, escolhendo $\theta \in \mathbb{R}$ de modo que $\alpha + k\theta = \pi$ (i.e., tomando $\theta = \frac{\pi - \alpha}{k}$), obtemos

$$\begin{aligned}\frac{|f(z_0+h)|}{|f(z_0)|} &\leq |1 + sr^k \operatorname{cis} \pi| + \frac{1}{2}sr^k \\ &= |1 - sr^k| + \frac{1}{2}sr^k \\ &= 1 - \frac{1}{2}sr^k < 1,\end{aligned}$$

sempre que $sr^k < 1$, i.e., $0 < r < \sqrt[k]{\frac{1}{s}}$. Com um tal r (e, logicamente, com o h correspondente), temos $|f(z_0 + h)| < |f(z_0)|$. □

Uma consequência imediata do teorema fundamental da álgebra é dada pelo corolário a seguir.

Corolário 3.25. *Se $f(X) = a_nX^n + \cdots + a_1X + a_0$ é um polinômio de coeficientes complexos e grau $n \geq 1$, então existem n números complexos $z_1, \ldots, z_n$ tais que*

$$f(X) = a_n(X - z_1)\ldots(X - z_n). \tag{3.8}$$

A expressão acima é a **forma fatorada** *do polinômio f.*

Prova. Façamos a prova por indução sobre o grau n de f, sendo o caso $n = 1$ imediato. Suponha, pois, $n > 1$ e o corolário válido para todo polinômio de coeficientes complexos e grau $n - 1$.

Se $z_1 \in \mathbb{C}$ é uma raiz de f, o teste da raiz garante a existência de um polinômio g, também de coeficientes complexos, tal que $f(X) = (X - z_1)g(X)$. Note que g tem grau $n - 1$ e coeficiente líder a_n; portanto, por hipótese de indução existem $z_2, \ldots, z_n \in \mathbb{C}$ tais que $g(X) = a_n(X - z_2)\ldots(X - z_n)$. Logo, $f(X) = (X - z_1)g(X) = a_n(X - z_1)(X - z_2)\ldots(X - z_n)$ e nada mais há a fazer. □

Uma variante do corolário acima é dada pelo resultado a seguir.

Corolário 3.26. *Se $f(X) = a_nX^n + \cdots + a_1X + a_0$ é um polinômio de coeficientes complexos e grau $n \geq 1$, então, dado $\alpha \in \mathbb{C}$, existem $z_1, \ldots, z_n \in \mathbb{C}$ tais que $f(z_k) = \alpha$, para $1 \leq k \leq n$.*

Prova. Aplique o corolário anterior ao polinômio $g(X) = f(X) - \alpha$. □

Voltando ao caso geral, seja $f(X) = a_nX^n + \cdots + a_1X + a_0$ um polinômio não nulo com coeficientes em $\mathbb{K}$. Se existirem elementos $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ para os quais

$$f(X) = a_n(X - \alpha_1)\ldots(X - \alpha_n),$$

também diremos que tal expressão é a **forma fatorada** de f sobre $\mathbb{K}$.

Uma vez que alguns dos α_j's podem aparecer repetidos, se considerarmos apenas os α_j distintos concluímos, após uma possível reenumeração dos mesmos, que existem $1 \leq m \leq n$ e $k_1, \ldots, k_m$ inteiros positivos tais que

$$f(X) = a_n(X - \alpha_1)^{k_1}\ldots(X - \alpha_m)^{k_m},$$

com $k_1 + \cdots + k_m = n$ e $\alpha_1, \ldots, \alpha_m$ elementos dois a dois distintos de $\mathbb{K}$.

Exemplo 3.27. *Dado $n > 1$ um natural, faça os seguintes itens:*

(a) Obtenha a forma fatorada do polinômio $f(X) = X^{n-1} + X^{n-2} + \cdots + X + 1$.

(b) Se $A_1A_2\ldots A_n$ é um polígono regular de n lados inscrito num círculo de raio 1, calcule o valor do produto $\overline{A_1A_2} \cdot \overline{A_1A_3} \cdot \ldots \cdot \overline{A_1A_n}$.

Solução.
(a) Uma vez que

$$(X - 1)f(X) = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1) = X^n - 1,$$

as raízes complexas de f são precisamente as raízes n−ésimas da unidade distintas de 1. Por (1.18), tais raízes são os números complexos $\omega, \omega^2, \ldots, \omega^{n-1}$, onde $\omega = \text{cis}\,\frac{2\pi}{n}$. Logo, a forma fatorada de f é

$$f(X) = (X-\omega)(X-\omega^2)\ldots(X-\omega^{n-1}).$$

(b) Suponha, sem perda de generalidade, que o círculo de raio 1 que circunscreve o polígono $A_1A_2\ldots A_n$ é o círculo unitário centrado na origem do plano complexo e que $A_1 = 1$ e $A_2 = \omega$, onde $\omega = \text{cis}\,\frac{2\pi}{n}$. Então, $A_j = \omega^{j-1}$ para $1 \leq j \leq n$, de sorte que

$$\begin{aligned}\overline{A_1A_2}\cdot\overline{A_1A_3}\cdot\ldots\cdot\overline{A_1A_n} &= |1-\omega||1-\omega^2|\ldots|1-\omega^{n-1}| \\ &= |(1-\omega)(1-\omega^2)\ldots(1-\omega^{n-1})| \\ &= |f(1)| = n.\end{aligned}$$

□

Problemas – Seção 3.3

1. Prove que a fórmula que dá as raízes de uma equação do segundo grau ainda é válida para calcular as raízes complexas de $aX^2 + bX + c$, com $a, b, c \in \mathbb{C}$, sendo $a \neq 0$.

2. * Se $f \in \mathbb{R}[X] \setminus \{0\}$ e $z \in \mathbb{C} \setminus \mathbb{R}$, prove que $f(z) = 0 \Leftrightarrow f(\overline{z}) = 0$. Conclua, a partir daí, que todo polinômio não nulo de coeficientes reais possui um número par de raízes complexas não reais.

3. Dê um exemplo para mostrar que o resultado do problema anterior não é mais válido caso f tenha coeficientes não reais.

4. * Prove que todo polinômio de coeficientes reais e grau ímpar tem um número ímpar de raízes reais. Em particular, um tal polinômio sempre tem pelo menos uma raiz real.

5. * Sejam $f \in \mathbb{Q}[X]$ um polinômio de grau n e $\alpha \neq 0$ uma raiz complexa de f. Dado $m \in \mathbb{Z}$, prove que existem $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Q}$ tais que
$$\alpha^m = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}. \quad (3.9)$$

6. Seja $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ um polinômio de coeficientes complexos e grau $n \geq 1$. Se $z \in \mathbb{C}$ é uma raiz de f, prove que
$$|z| \leq \max\left\{1, \frac{nA}{|a_n|}\right\},$$
onde $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$.

7. * Seja $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ um polinômio de coeficientes inteiros tal que $a_n \geq 1$, e $k > 2$ um inteiro tal que $|a_i| \leq k$, para $0 \leq i < n$. Se z é uma raiz complexa de f, prove que $\text{Re}(z) < 1 + \frac{k}{2}$.

8. Um polinômio f sobre $\mathbb{C}$ da forma $f(X) = aX^4 + bX^3 + cX^2 + bX + a$, com $a \neq 0$, é denominado **recíproco** de quarto grau. Calcule suas raízes e, em seguida, formule e resolva o problema análogo para polinômios de grau seis.

9. (Canadá.) Seja f um polinômio de grau n, tal que $f(k) = \frac{k}{k+1}$, para todo inteiro $0 \leq k \leq n$. Calcule $f(n+1)$.

10. Suponha que as raízes complexas do polinômio $X^3 + pX^2 + qX + r$ sejam todas reais e positivas. Mostre que tais raízes são os comprimentos dos lados de um triângulo se, e só se, $p^3 - 4pq + 8r > 0$.

11. Para $n > 2$ inteiro, prove que

$$\operatorname{sen}\frac{\pi}{n}\operatorname{sen}\frac{2\pi}{n}\operatorname{sen}\frac{3\pi}{n}\ldots\operatorname{sen}\frac{(n-1)\pi}{n}=\frac{n}{2^{n-1}}.$$

12. Dado um inteiro positivo m, prove que:

    (a) $\operatorname{sen}\frac{\pi}{2m}\operatorname{sen}\frac{2\pi}{2m}\ldots\operatorname{sen}\frac{(m-1)\pi}{2m}=\frac{\sqrt{m}}{2^{m-1}}$.

    (b) $\operatorname{sen}\frac{\pi}{2m+1}\operatorname{sen}\frac{2\pi}{2m+1}\ldots\operatorname{sen}\frac{m\pi}{2m+1}=\frac{\sqrt{2m+1}}{2^m}$.

13. (Romênia.) Encontre todos os polinômios não constantes p, de coeficientes reais e tais que $p(X^2)=p(X)p(X-1)$.

3.4 Raízes múltiplas

Seja f um polinômio de coeficientes complexos. No que segue, convencionamos dizer que $z \in \mathbb{C}$ é raiz de multiplicidade zero de f se z não for raiz de f. Queremos, nesta seção, encontrar um critério que nos permita decidir se z é ou não raiz múltipla de f e, caso o seja, calcular sua multiplicidade. Para tanto, precisamos da definição a seguir.

Definição 3.28. *Para um polinômio $f(X)=a_nX^n+\cdots+a_1X+a_0 \in \mathbb{C}[X]$, definimos a* **derivada** *$f' \in \mathbb{C}[X]$ de f como o polinômio*

$$f'(X)=na_nX^{n-1}+(n-1)a_{n-2}X^{n-2}+\cdots+2a_2X+a_1$$

se $\partial f > 0$. Senão, definimos $f'=0$.

A regra para a obtenção da derivada de um polinômio é bastante simples: a derivada de um polinômio constante é o polinômio identicamente nulo; a derivada de um polinômio de grau $n \geq 1$ é obtida *apagando* seu termo constante e efetuando, para $1 \leq k \leq n$, a troca de monômios

$$a_kX^k \mapsto ka_kX^{k-1}.$$

A proposição a seguir lista as principais propriedades básicas de derivadas de polinômios.

Proposição 3.29. *Para $f_1,\ldots,f_k \in \mathbb{C}[X]$ e $a_1,\ldots,a_k \in \mathbb{C}$, temos:*

(a) $\left(\sum_{i=1}^k a_if_i\right)'=\sum_{i=1}^k a_if_i'$.

(b) $\left(\prod_{i=1}^k f_i\right)'=\sum_{i=1}^k f_1\ldots f_i'\ldots f_k$.

Prova.
(a) Imediato, por indução sobre $k \geq 1$. (Observe que os casos iniciais são $k=1$ e $k=2$.)

(b) Considere, primeiro, dois polinômios f e g dados por

$$f(X)=a_nX^n+\cdots+a_1X+a_0 \;\text{ e }\; g(X)=b_mX^m+\cdots+b_1X+b_0.$$

Omitindo X quando conveniente, segue de (a) que

$$(fg)'=\left[\left(\sum_{j=0}^n a_jX^j\right)g\right]'=\left(\sum_{j=0}^n a_jX^jg\right)'=\sum_{j=0}^n(a_jX^jg)'.$$

Por outro lado,

$$\begin{aligned}(a_jX^jg)' &= \left(a_jX^j\sum_{i=0}^m b_iX^i\right)'=\left(\sum_{i=0}^m a_jb_iX^{j+i}\right)'=\sum_{i=0}^m(a_jb_iX^{j+i})'\\ &=\sum_{i=0}^m(j+i)a_jb_iX^{j+i-1}\\ &=\sum_{i=0}^m ja_jb_iX^{j+i-1}+\sum_{i=0}^m ia_jb_iX^{j+i-1}\\ &=ja_jX^{j-1}\sum_{i=0}^m b_iX^i+a_jX^j\sum_{i=1}^m ib_iX^{i-1}\\ &=(a_jX^j)'g+(a_jX^j)g'.\end{aligned}$$

Portanto, voltando à expressão anterior para $(fg)'$, obtemos

$$\begin{aligned}(fg)' &= \sum_{j=0}^{n}[(a_jX^j)'g + a_jX^jg'] \\ &= \left(\sum_{j=0}^{n}(a_jX^j)'\right)g + \left(\sum_{j=0}^{n}a_jX^j\right)g' \\ &= \left(\sum_{j=0}^{n}a_jX^j\right)'g + fg' \\ &= f'g + fg',\end{aligned}$$

onde utilizamos novamente o item (a) na penúltima igualdade. Por fim, a extensão para k polinômios $f_1, \ldots, f_k$ é imediata por indução. □

Corolário 3.30. *Dados $g \in \mathbb{C}[X]$ e $n \in \mathbb{N}$, se $f(X) = g(X)^n$, então $f'(X) = ng(X)^{n-1}g'(X)$. Em particular, se $f(X) = (X - a)^n$, então $f'(X) = n(X - a)^{n-1}$.*

Prova. Fazendo $k = n$ e $f_1 = \cdots = f_n = g$ no item (b) da proposição anterior, obtemos

$$f'(X) = \sum_{i=1}^{n} g(X)^{n-1}g'(X) = ng(X)^{n-1}g'(X),$$

O caso particular segue daí, pondo $g(X) = X - a$. □

A proposição a seguir vincula a multiplicidade de uma raiz de um polinômio às derivadas do mesmo.

Proposição 3.31. *Seja f um polinômio não nulo de coeficientes complexos e z um complexo dado.*

(a) Se z for raiz de multiplicidade $m \geq 1$ de f, então z é raiz de multiplicidade $m - 1$ de f'.

(b) Se z for raiz de f e for raiz de multiplicidade $m - 1$ de f', então z é raiz de multiplicidade m de f.

Prova.
(a) Seja $f(X) = (X - z)^m g(X)$, com $g(z) \neq 0$. O item (b) da proposição anterior e seu corolário nos dão

$$\begin{aligned}f'(X) &= m(X - z)^{m-1}g(X) + (X - z)^m g'(X) \\ &= (X - z)^{m-1}[mg(X) + (X - z)g'(X)].\end{aligned}$$

Portanto, sendo $h(X) = mg(X) + (X - z)g'(X)$, temos $h(z) = mg(z) \neq 0$ e $f'(X) = (X - z)^{m-1}h(X)$. Pela definição, segue que z é raiz de multiplicidade $m - 1$ de f'.

(b) Seja $f(X) = (X - z)^k g(X)$, com $g(z) \neq 0$ e $k \geq 1$. Pelo item (a), a multiplicidade de α como raiz de f' é $k - 1$, de modo que $k - 1 = m - 1$ e, daí, $k = m$. □

Corolário 3.32. *Se $z \in \mathbb{C}$ e $f \in \mathbb{C}[X] \setminus \{0\}$, então z é raiz múltipla de f se, e só se, $f(z) = f'(z) = 0$.*

Prova. Imediata, a partir da proposição anterior. □

Exemplo 3.33. *Prove que, para todo inteiro positivo n, o polinômio*

$$1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$$

não tem raízes múltiplas.

Prova. Seja $f(X) = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$, e suponha que f tem uma raiz múltipla z. Então, pelo corolário anterior, temos $f(z) = f'(z) = 0$. Agora, uma vez que $f(X) = f'(X) + \frac{X^n}{n!}$, seguiria daí que

$$0 = f(z) = f'(z) + \frac{z^n}{n!},$$

i.e., $z = 0$. Mas, como $f(0) = 1 \neq 0$, chegamos a uma contradição. □

A fim de refinar o corolário anterior precisamos, inicialmente, generalizar a definição 3.28.

Definição 3.34. *Para $f \in \mathbb{C}[X] \setminus \{0\}$, definimos a $k-$ésima derivada de f, denotada $f^{(k)}$, por*

$$f^{(k)} = \begin{cases} f, & \text{se } k = 0 \\ \left(f^{(k-1)}\right)', & \text{se } k \geq 1 \end{cases}.$$

Segue da definição acima que $f^{(1)} = (f^{(0)})' = f'$; daí, $f^{(2)} = (f^{(1)})' = (f')'$, de sorte que denotamos $f^{(2)} = f''$. Analogamente, sempre que conveniente, denotamos $f^{(3)} = f'''$, etc.

Se $\partial f = n$ e $0 \leq k \leq n$, então uma fácil indução garante que $\partial f^{(k)} \leq n - k$; em particular, $\partial f^{(n)} = 0$ e, daí, $f^{(n+1)} = f^{(n+2)} = \cdots = 0$.

Corolário 3.35. *Se $z \in \mathbb{C}$ e $f \in \mathbb{C}[X] \setminus \{0\}$, então z é raiz de multiplicidade $m \geq 1$ de f se, e só se,*

$$f(z) = \cdots = f^{(m-1)}(z) = 0 \text{ e } f^{(m)}(z) \neq 0.$$

Prova. Suponha, primeiro, que z seja raiz de multiplicidade m de f. Repetidas aplicações do item (a) da proposição 3.31 nos dão, por um lado,

$$f(z) = \cdots = f^{(m-1)}(z) = 0$$

e, por outro, que z é raiz de multiplicidade zero de $f^{(m)}$, i.e., que $f^{(m)}(z) \neq 0$.

Reciprocamente, suponha a condição do enunciado satisfeita e sejam $k \in \mathbb{N}$ e $g \in \mathbb{C}[X]$ tais que $f(X) = (X - z)^k g(X)$, com $g(z) \neq 0$. Novamente pelo item (a) da proposição 3.31, para $0 \leq j \leq k$ temos que z é raiz de multiplicidade $k - j$ de $f^{(j)}$. Em particular,

$$f(z) = \cdots = f^{(k-1)}(z) = 0 \text{ e } f^{(k)}(z) \neq 0.$$

Agora

$$f(z) = \cdots = f^{(m-1)}(z) = 0 \Rightarrow k \leq m$$

e

$$f^{(m)}(z) \neq 0 \Rightarrow k \geq m.$$

□

Nosso propósito, no restante desta seção, é mostrar que, se $f \in \mathbb{C}[X] \setminus \{0\}$ tem grau n e $z \in \mathbb{C}$, então f é totalmente determinado pelos valores $f^{(k)}(z)$, para $0 \leq k \leq n$. Antes, contudo, precisamos de mais duas consequências da proposição 3.31.

Corolário 3.36. *Seja $f \in \mathbb{C}[X]$ tal que $f = 0$ ou $\partial f \leq n$. Se $z \in \mathbb{C}$ é tal que $f(z) = \cdots = f^{(n)}(z) = 0$, então $f = 0$.*

Prova. Se $f \neq 0$, o corolário anterior garante que z é raiz de multiplicidade pelo menos $n + 1$ de f. Mas, como $\partial f \leq n$, chegamos a uma contradição. □

Corolário 3.37. *Sejam $f, g \in \mathbb{C}[X] \setminus \{0\}$, com $\partial f, \partial g \leq n$. Se existe $z \in \mathbb{C}$ tal que*

$$f(z) = g(z), \ \ldots, f^{(n)}(z) = g^{(n)}(z),$$

então $f = g$.

Prova. Basta aplicar o corolário anterior a $f - g$, notando (a partir da definição 3.34 e por indução sobre $k \geq 1$) que

$$(f - g)^{(k)}(X) = f^{(k)}(X) - g^{(k)}(X).$$

□

O resultado a seguir é conhecido como a **fórmula de Taylor** para polinômios, sendo uma consequência imediata do corolário acima.

Teorema 3.38. *Se $z \in \mathbb{C}$ e $f \in \mathbb{C}[X] \setminus \{0\}$ tem grau n, então*

$$f(X) = f(z) + \frac{f^{(1)}(z)}{1!}(X - z) + \cdots + \frac{f^{(n)}(z)}{n!}(X - z)^n. \qquad (3.10)$$

Prova. Defina

$$g(X) = f(z) + \frac{f'(z)}{1!}(X - z) + \cdots + \frac{f^{(n)}(z)}{n!}(X - z)^n.$$

Como $f \neq 0$, segue do corolário 3.36 que ao menos um dentre os números $f(z)$, $f'(z)$, ..., $f^{(n)}(z)$ é não nulo; portanto, $g \neq 0$. Por outro lado, é imediato verificar que, para $0 \leq k \leq n$, temos

$$g^{(k)}(X) = \sum_{j=k}^{n} \frac{f^{(j)}(z)}{(j-k)!}(X - z)^{j-k}$$

e, daí, que

$$f(z) = g(z),\ f'(z) = g'(z),\ \ldots,\ f^{(n)}(z) = g^{(n)}(z).$$

Mas, como f e g têm graus menores ou iguais a n, segue do corolário anterior que $f = g$. □

Exemplo 3.39. *Seja $f \in \mathbb{R}[X] \setminus \{0\}$ e $a \in \mathbb{R}$ tal que $f(a) = 0$ e $f^{(k)}(a) \geq 0$, para todo $k \geq 1$. Prove que f não possui raízes no intervalo $(a, +\infty)$.*

Prova. Pela fórmula de Taylor, temos

$$f(X) = \frac{f'(a)}{1!}(X - a) + \cdots + \frac{f^{(n)}(a)}{n!}(X - a)^n,$$

onde $n = \partial f$. Mas, como $f \neq 0$, ao menos uma das derivadas $f^{(k)}(a)$, para $1 \leq k \leq n$, é positiva. Assim, sendo $x > a$ um número real e $f^{(j)}(a) > 0$, temos

$$\begin{aligned} f(x) &= \frac{f'(a)}{1!}(x - a) + \cdots + \frac{f^{(n)}(a)}{n!}(x - a)^n \\ &\geq \frac{f^{(j)}(a)}{j!}(X - a)^j > 0. \end{aligned}$$

□

Problemas – Seção 3.4

1. Ache todos os valores inteiros de a para os quais o polinômio $f(X) = X^3 - aX^2 + 5X - 2$ possui raízes múltiplas.

2. * Generalize parcialmente o item (a) da proposição 3.31, mostrando que, se $f, g \in \mathbb{C}[X]$ são tais que $g(X)^2 \mid f(X)$, então $g(X) \mid f'(X)$.

3. * Para $z_1, \ldots, z_n \in \mathbb{C}$, seja $f(X) = (X - z_1) \ldots (X - z_n)$. Prove que, para $z \in \mathbb{C} \setminus \{z_1, \ldots, z_n\}$, temos
$$\frac{f'(z)}{f(z)} = \sum_{j=1}^{n} \frac{1}{z - z_j}.$$

4. * Generalize o problema anterior provando que, se $f_1, \ldots, f_k \in \mathbb{C}[X]$, $f = f_1 \ldots f_k$ e $z \in \mathbb{C}$ não é raiz de f, então
$$\frac{f'(z)}{f(z)} = \frac{f_1'(z)}{f_1(z)} + \cdots + \frac{f_k'(z)}{f_k(z)}.$$

5. (Estados Unidos.) Para cada conjunto não vazio e finito S de números reais, sejam $\sigma(S)$ e $\pi(S)$, respectivamente, a soma e o produto de seus elementos. Prove que
$$\sum_{\emptyset \neq S \subset I_n} \frac{\sigma(S)}{\pi(S)} = n^2 + 2n - \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right)(n + 1).$$

6. Prove o seguinte teorema de Gauss: se $f(X) = a_nX^n + \cdots + a_1X + a_0$ é um polinômio de grau maior que 1 e coeficientes complexos, então as raízes de f' estão contidas no menor polígono convexo (possivelmente degenerado) do plano complexo que tem as raízes de f como vértices.

7. * Se f é um polinômio de coeficientes inteiros e grau n e $a \in \mathbb{Z}$, prove que $\frac{f^{(j)}(a)}{j!} \in \mathbb{Z}$, para $0 \leq j \leq n$.

8. Seja f um polinômio de coeficientes inteiros e p um primo que não divide seu coeficiente líder. Se m é um natural tal que

$$f(m) \equiv 0 \pmod{p} \quad \text{e} \quad f'(m) \not\equiv 0 \pmod{p},$$

prove que, para todo $k \in \mathbb{N}$, existe $m_k \in \mathbb{N}$ tal que

$$f(m_k) \equiv 0 \pmod{p^k}.$$

CAPÍTULO 4

Relações entre Coeficientes e Raízes

Nosso propósito neste capítulo é formalizar e provar algumas relações importantes entre as raízes de um polinômio em uma indeterminada, resultados estes denominados genericamente de *relações entre coeficientes e raízes* de um polinômio. Também, discutimos um importante teorema de Newton sobre polinômios simétricos, o qual se revelará de importância central para a discussão do capítulo 8.

Para o que segue, lembre-se de que $\mathbb{K}$ denota $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

4.1 Polinômios em várias indeterminadas

Fixado $n \in \mathbb{N}$, um **polinômio** f **a** n **indeterminadas** sobre $\mathbb{K}$ é uma soma de monômios do tipo

$$a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n},$$

onde $a_{i_1\ldots i_n} \in \mathbb{K}$ e $i_1, \ldots, i_n$ variam em $\mathbb{Z}_+$, sendo $a_{i_1\ldots i_n} = 0$ para quases todas (i.e., para todas, exceto um número finito de) sequências $(i_1, \ldots, i_n)$ de inteiros não negativos. Nesse caso, escrevemos

$$f = f(X_1, X_2, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n}.$$

O **grau** de um polinômio f como acima é o maior valor possível para a soma $i_1 + \cdots + i_n$, tal que $a_{i_1\ldots i_n} \neq 0$.

Denotamos por $\mathbb{K}[X_1, \ldots, X_n]$ o conjunto dos polinômios a n indeterminadas sobre $\mathbb{K}$. Sobre tal conjunto definimos, de maneira óbvia, operações

$$+ : \mathbb{K}[X_1, \ldots, X_n] \times \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}[X_1, \ldots, X_n]$$

e

$$\cdot : \mathbb{K}[X_1, \ldots, X_n] \times \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}[X_1, \ldots, X_n],$$

respectivamente denominadas **adição** e **multiplicação**, as quais se reduzem às operações de adição e multiplicação sobre $\mathbb{K}[X]$ quando $n = 1$ e continuam gozando das mesmas propriedades dessas operações. Por exemplo, se $f(X_1, X_2) = X_1^2 + X_1X_2 + X_2^3$ e $g(X_1, X_2) = X_1^3 - \sqrt{2}X_1X_2$, então

$$f(X_1, X_2) + g(X_1, X_2) = X_1^2 + (1 - \sqrt{2})X_1X_2 + X_1^3 + X_2^3$$

e

$$\begin{aligned} f(X_1, X_2) \cdot g(X_1, X_2) &= X_1^5 - \sqrt{2}X_1^3X_2 + X_1^4X_2 - \sqrt{2}X_1^2X_2^2 \\ &+ X_1^3X_2^3 - \sqrt{2}X_1X_2^4. \end{aligned}$$

Dado $f \in \mathbb{K}[X_1, \ldots, X_n]$, podemos considerar f como um polinômio em X_i, com coeficientes em $\mathbb{K}[X_1, \ldots, \widehat{X_i}, \ldots, X_n]$, onde usamos o *circunflexo* $\wedge$ sobre X_i para indicar que todas as indeterminadas, menos X_i, estão presentes. Por exemplo, seja

$$f(X_1, X_2, X_3) = X_1^3X_2X_3^4 - X_1^3 - 5X_1X_2 + 10X_1X_2^5X_3^2,$$

um polinômio em $\mathbb{K}[X_1, X_2, X_3]$; escrevendo

$$f(X_1, X_2, X_3) = X_1^3X_2 \cdot X_3^4 + 10X_1X_2^5 \cdot X_3^2 - (X_1^3 + 5X_1X_2),$$

consideramos f como um polinômio em X_3, cujos coeficientes estão em $\mathbb{K}[X_1, X_2]$.

Se $f, g \in \mathbb{K}[X_1, \ldots, X_n]$ são dados por

$$f(X_1, X_2, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

e

$$g(X_1, X_2, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} b_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n},$$

dizemos que f e g são *iguais* quando $a_{i_1\ldots i_n} = b_{i_1\ldots i_n}$, para todas as escolhas possíveis de índices $i_1, \ldots, i_n \in \mathbb{Z}_+$.

Fixados $x_1, x_2 \ldots, x_n \in \mathbb{K}$, definimos o elemento $f(x_1, x_2, \ldots, x_n) \in \mathbb{K}$ por

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1\ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

A proposição a seguir nos dá uma relação entre tais elementos de $\mathbb{K}$ e a noção de igualdade de polinômios em várias indeterminadas.

Proposição 4.1. *Sejam $f, g \in \mathbb{K}[X_1, \ldots, X_n]$. Se $A_1, \ldots, A_n \subset \mathbb{K}$ são conjuntos infinitos, então*

$$f = g \Leftrightarrow f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n),$$

para todos $x_1 \in A_1$, $x_2 \in A_2$, ..., $x_n \in A_n$.

Prova. Se $f = g$, é claro que $f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n)$, para todos $x_1, x_2, \ldots, x_n \in \mathbb{K}$ e, em particular, para $x_1 \in A_1$, $x_2 \in A_2$, ..., $x_n \in A_n$.

Reciprocamente, suponhamos que esta última condição seja satisfeita e provemos que $f = g$ usando indução sobre o número n de

indeterminadas. Já temos a validade da proposição para $n = 1$, pelo corolário 3.10. Por hipótese de indução, suponha o resultado válido para polinômios em $n-1$ indeterminadas e escreva

$$\begin{cases} f(X_1, X_2, \ldots, X_n) = \sum_{j=0}^{m} f_j(X_2, \ldots, X_n) X_1^j \\ g(X_1, X_2, \ldots, X_n) = \sum_{j=0}^{p} g_j(X_2, \ldots, X_n) X_1^j \end{cases}, \tag{4.1}$$

com $f_i, g_j \in \mathbb{K}[X_2, \ldots, X_n]$ para todos $0 \le i \le m$, $0 \le j \le p$.

Fixados $x_2 \in A_2, \ldots, x_n \in A_n$, temos por hipótese de indução que

$$f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n),$$

para todo $x_1 \in A_1$, i.e., que

$$\sum_{j=0}^{m} f_j(x_2, \ldots, x_n) x_1^j = \sum_{j=0}^{p} g_j(x_2, \ldots, x_n) x_1^j,$$

para todo $x_1 \in A_1$. Como o conjunto A_1 é infinito, aplicando o corolário 3.10 aos polinômios

$$f(X_1, x_2, \ldots, x_n) = \sum_{j=0}^{m} f_j(x_2, \ldots, x_n) X_1^j$$

e

$$g(X_1, x_2, \ldots, x_n) = \sum_{j=0}^{p} g_j(x_2, \ldots, x_n) X_1^j,$$

concluímos que $m = p$ e

$$f_j(x_2, \ldots, x_n) = g_j(x_2, \ldots, x_n) \tag{4.2}$$

para $0 \le j \le m$. Mas, como os elementos $x_2 \in A_2, \ldots, x_n \in A_n$ fixados foram escolhidos arbitrariamente, concluímos que (4.2) é válida para todos $x_2 \in A_2, \ldots, x_n \in A_n$. Portanto, pela hipótese de indução segue que $f_j = g_j$ para $0 \le j \le m$, e (4.1) garante que $f = g$. □

Observação 4.2. *Doravante, ao lidarmos com polinômios f em duas indeterminadas, escreveremos em geral $f(X, Y)$ em vez de $f(X_1, X_2)$. Uma notação análoga será usada para polinômios f em três indeterminadas: escreveremos $f(X, Y, Z)$ em vez de $f(X_1, X_2, X_3)$.*

Exemplo 4.3. *Escreva o polinômio $(X + Y + Z)^3 - (X^3 + Y^3 + Z^3)$ como produto de polinômios de grau 1.*

Solução. Fixe $y, z \in \mathbb{R}^*$, com $y \neq z$, e considere o polinômio em X

$$g(X) = f(X, y, z) = (X + y + z)^3 - X^3 - (y^3 + z^3).$$

Uma vez que

$$f(-y, y, z) = (-y + y + z)^3 - ((-y)^3 + y^3 + z^3) = 0,$$

temos pelo teste da raiz que o polinômio $f(X, y, z)$ (em X) é divisível por $X - (-y) = X + y$. Analogamente, f é divisível por $X + z$ e, como $\partial g = 2$, o item (c) da proposição 3.3 garante que

$$f(X, y, z) = \alpha(X + y)(X + z),$$

sendo $\alpha \in \mathbb{R}$ a determinar. Avaliando a igualdade acima em 0, obtemos

$$\alpha yz = f(0, y, z) = (y + z)^3 - (y^3 + z^3) = 3yz(y + z),$$

de forma que $\alpha = 3(y + z)$. Logo,

$$f(X, y, z) = 3(y + z)(X + y)(X + z)$$

e, daí, $f(x, y, z) = 3(y+z)(x+y)(x+z)$, para todos $x \in \mathbb{R}$ e $y, z \in \mathbb{R}^*$, com $y \neq z$. Pela proposição 4.1, segue então que

$$f(X, Y, Z) = 3(Y + Z)(X + Y)(X + Z).$$

□

Problemas – Seção 4.1

1. * Se $f \in \mathbb{K}[X_1, \ldots, X_n]$ é não nulo, prove que existem conjuntos infinitos $A_1, \ldots, A_n \subset \mathbb{K}$ tais que $f(x_1, \ldots, x_n) \neq 0$, para todos $x_1 \in A_1, \ldots, x_n \in A_n$.

2. Faça os seguintes itens:

   (a) Prove que o polinômio $(X-Y)^5 + (Y-Z)^5 + (Z-X)^5$ é divisível pelo polinômio $(X-Y)(Y-Z)(Z-X)$.

   (b) Fatore o polinômio $(X-Y)^5 + (Y-Z)^5 + (Z-X)^5$.

3. Fatore o polinômio $(X+Y+Z)^5 - X^5 - Y^5 - Z^5$ como produto de três polinômios de grau 1 e um polinômio de grau 2.

4.2 Polinômios simétricos

O objeto de estudo dessa seção é isolado na definição a seguir.

Definição 4.4. *Um polinômio $f \in \mathbb{K}[X_1, \ldots, X_n]$ é* **simétrico** *quando*

$$f(X_1, X_2, \ldots, X_n) = f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}),$$

para toda permutação σ de I_n.

Para entender melhor a definição acima, considere os polinômios $f, g \in \mathbb{K}[X, Y]$, dados por

$$f(X,Y) = X^2 + Y^2 - XY + X + Y \quad \text{e} \quad g(X,Y) = X^3 + Y^3 - X.$$

O primeiro é simétrico mas o segundo não, uma vez que

$$f(Y,X) = Y^2 + X^2 - YX + Y + X = f(X,Y),$$

mas

$$g(Y,X) = Y^3 + X^3 - Y \neq g(X,Y).$$

Um certo conjunto de polinômios simétricos, ditos *elementares*, merece especial atenção. Explicitamos tais polinômios na definição a seguir.

Definição 4.5. *Para $0 \leq j \leq n$, o j−ésimo* **polinômio simétrico elementar** *em $X_1, \ldots, X_n$, denotado $s_j = s_j(X_1, \ldots, X_n)$, é definido como*

$$s_j(X_1, \ldots, X_n) = \begin{cases} 1, & \text{se } j = 0 \\ \sum_{1 \leq i_1 < \cdots < i_j \leq n} X_{i_1} X_{i_2} \ldots X_{i_j}, & \text{se } 1 \leq j \leq n \end{cases}.$$

No caso $n = 3$, por exemplo, temos

$$s_0 = 1, \quad s_1 = X + Y + Z, \quad s_2 = XY + YZ + XZ, \quad s_3 = XYZ.$$

Para um natural n qualquer, não é difícil provar que s_j é de fato simétrico. Por outro lado, a importância dos polinômios simétricos elementares reside na proposição a seguir, sendo as relações (4.3) conhecidas como as **relações de Girard**[1] entre coeficientes e raízes de um polinômio.

Proposição 4.6. *Se $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{K}[X] \setminus \mathbb{K}$ se fatora completamente sobre $\mathbb{K}$, com raízes $\alpha_1, \ldots, \alpha_n$, então, para $1 \leq j \leq n$, temos*

$$s_j(\alpha_1, \ldots, \alpha_n) = (-1)^j \frac{a_{n-j}}{a_n}. \tag{4.3}$$

Prova. Por simplicidade de notação, denote $s_j(\alpha_1, \ldots, \alpha_n)$ simplesmente por $s_j(\alpha_i)$. Escrevendo $f(X) = a_n(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$ e expandindo os parênteses, obtemos

$$f(X) = a_n X^n - a_n s_1(\alpha_i) X^{n-1} + a_n s_2(\alpha_i) X^{n-2} - \cdots + a_n(-1)^n s_n(\alpha_i).$$

Igualando os coeficientes correspondentes nessa expressão para f e naquela do enunciado, obtemos o resultado desejado. □

[1] Após Albert Girard, matemático francês do século XVII.

A fim de ilustrar o que a proposição acima diz e o que ela não diz, considere as raízes complexas α, β e γ do polinômio $f(X) = X^3 - 2X^2 + 1$. Pelas relações de Girard, temos

$$\alpha + \beta + \gamma = 2, \quad \alpha\beta + \alpha\gamma + \beta\gamma = 0 \text{ e } \alpha\beta\gamma = -1.$$

Porém, vale observar que tais relações não trazem informação suficiente para calcularmos α, β e γ; de fato, ao tentarmos resolver o sistema formado pelas igualdades acima, recaímos nas equações polinomiais $f(\alpha) = 0$, $f(\beta) = 0$ e $f(\gamma) = 0$. Senão, vejamos: multiplicando ambos os membros da segunda relação por α, obtemos

$$\alpha^2(\beta + \gamma) + \alpha\beta\gamma = 0;$$

substituindo nessa igualdade $\beta + \gamma$ por $2 - \alpha$ e $\alpha\beta\gamma$ por -1, segue que

$$\alpha^2(2 - \alpha) - 1 = 0.$$

Nas notações da proposição acima, nos referimos a $s_j(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}$ como a j−ésima **soma simétrica elementar** das raízes de f. Sempre que $\alpha_1, \ldots, \alpha_n$ estiverem subentendidos e não houver perigo de confusão com o polinômio simétrico elementar $s_j = s_j(X_1, \ldots, X_n)$, denotaremos a soma simétrica elementar $s_j(\alpha_1, \ldots, \alpha_n)$ simplesmente por s_j.

Apresentamos, a seguir, uma série de exemplos que ilustram a variedade de situações em que podemos empregar as relações de Girard.

Exemplo 4.7. *Seja $f(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$ um polinômio de coeficientes reais, tal que $a_{n-1}^2 < 2a_{n-2}$. Prove que f tem ao menos duas raízes complexas não reais.*

Prova. Por contradição, suponha que $a_{n-1}^2 < 2a_{n-2}$ mas ao menos $n - 1$ dentre as raízes complexas de f sejam reais. Como f tem coeficientes reais, o resultado do problema 2, página 74, garante que

todas as raízes complexas de f são reais. Mas, se $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ são tais raízes, as relações de Girard fornecem

$$\sum_{i=1}^{n} \alpha_i = -a_{n-1} \text{ e } \sum_{i<j} \alpha_i\alpha_j = a_{n-2}.$$

A partir daí, temos

$$\sum_{i=1}^{n} \alpha_i^2 = \left(\sum_{i=1}^{n} \alpha_i\right)^2 - 2\sum_{i<j} \alpha_i\alpha_j = a_{n-1}^2 - 2a_{n-2} < 0,$$

o que nos fornece a contradição desejada. □

Exemplo 4.8. *Sejam a, b e c números reais não nulos, tais que $a + b + c = 0$. Prove que*

$$\frac{a^5 + b^5 + c^5}{5} = \left(\frac{a^3 + b^3 + c^3}{3}\right)\left(\frac{a^2 + b^2 + c^2}{2}\right).$$

Prova. Se $f(X) = (X-a)(X-b)(X-c)$, então a condição $a+b+c = 0$ garante que $f(X) = X^3 + sX - t$, onde $s = ab + ac + bc$ e $t = abc$. Mas, como $f(a) = 0$, temos $a^3 = -sa + t$ e, analogamente, $b^3 = -sb + t$ e $c^3 = -sc + t$. Somando membro a membro essas três igualdades e usando novamente a condição $a + b + c = 0$, obtemos

$$a^3 + b^3 + c^3 = -s(a + b + c) + 3t = 3t.$$

Para manipular adequadamente a soma $a^5 + b^5 + c^5$, comece multiplicando ambos os membros das igualdades $a^3 = -sa + t$, $b^3 = -sb + t$ e $c^3 = -sc + t$ respectivamente por a^2, b^2 e c^2; em seguida, some membro a membro os resultados para obter

$$a^5 + b^5 + c^5 = -s(a^3 + b^3 + c^3) + t(a^2 + b^2 + c^2).$$

Substituindo, na igualdade acima, a expressão para $a^3 + b^3 + c^3$ obtida no parágrafo anterior e observando que

$$a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + ac + bc) = -2s,$$

chegamos à igualdade

$$a^5 + b^5 + c^5 = -s \cdot 3t + t(-2s) = -5st.$$

A igualdade do enunciado é, agora, óbvia. □

Exemplo 4.9. *As raízes do polinômio $f(X) = X^3 - 7X^2 + 14X - 6$ são os comprimentos dos lados de um triângulo. Calcule a área do mesmo.*

Solução. Sejam a, b e c as raízes de f e A a área do triângulo tendo tais raízes por lados. A fórmula de Herão para a área de triângulos (proposição 7.30 de [11]) nos dá

$$A^2 = p(p-a)(p-b)(p-c),$$

onde p é o semi-perímetro do triângulo. Por outro lado, pelas relações de Girard, temos

$$p = \frac{1}{2}(a+b+c) = \frac{1}{2}s_1(a,b,c) = \frac{7}{2},$$

de maneira que

$$A^2 = \frac{7}{2}\left(\frac{7}{2} - a\right)\left(\frac{7}{2} - b\right)\left(\frac{7}{2} - c\right).$$

Usando agora a forma fatorada de f, temos

$$f(X) = (X-a)(X-b)(X-c) = X^3 - 7X^2 + 14X - 6$$

e, daí,

$$\begin{aligned} f\left(\frac{7}{2}\right) &= \left(\frac{7}{2} - a\right)\left(\frac{7}{2} - b\right)\left(\frac{7}{2} - c\right) \\ &= \left(\frac{7}{2}\right)^3 - 7\left(\frac{7}{2}\right)^2 + 14\left(\frac{7}{2}\right) - 6 \\ &= \frac{1}{8}. \end{aligned}$$

Logo,

$$A^2 = \frac{7}{2} \cdot f\left(\frac{7}{2}\right) = \frac{7}{2} \cdot \frac{1}{8} = \frac{7}{16},$$

de sorte que $A = \frac{\sqrt{7}}{4}$. □

Exemplo 4.10 (Romênia). *Sejam a, b, c e d números reais tais que*

$$a = \sqrt{4 - \sqrt{5-a}}, \quad b = \sqrt{4 + \sqrt{5-b}},$$

$$c = \sqrt{4 - \sqrt{5+c}} \text{ e } d = \sqrt{4 + \sqrt{5+d}}.$$

Calcule os possíveis valores do produto abcd.

Solução. Veja que $a^2 = 4 - \sqrt{5-a}$, de sorte que $(a^2-4)^2 = 5 - a$ ou, ainda, $a^4 - 8a^2 + a + 11 = 0$. Analogamente, obtemos $b^4 - 8b^2 + b + 11 = 0$, de maneira que a e b são raízes do polinômio

$$f(X) = X^4 - 8X^2 + X + 11.$$

Do mesmo modo, concluímos que c e d são raízes do polinômio $X^4 - 8X^2 - X + 11$ e segue, daí, que $-c$ e $-d$ também são raízes de f.

Portanto, a, b, $-c$ e $-d$ são todos raízes de f e, se soubermos que tais raízes são duas a duas distintas, concluiremos que elas são todas as raízes do polinômio f; daí, as relações de Girard nos darão

$$abcd = ab(-c)(-d) = 11.$$

Para o que falta, se tivéssemos, por exemplo, $a = b$, teríamos $\sqrt{4 - \sqrt{5-a}} = \sqrt{4 + \sqrt{5-a}}$ e, assim, $a = 5$. Mas, como $5 \neq \sqrt{4 - \sqrt{5-5}}$, temos $a \neq b$. Analogamente, provamos que $c \neq d$; por fim, como $-c, -d < 0 < a, b$, nada mais há a fazer. □

Exemplo 4.11 (Romênia). *Se $x_1, x_2, \ldots, x_n$ são reais positivos tais que $x_1 x_2 \ldots x_n = 1$, prove que*

$$\sum_{j=1}^{n} \frac{1}{n - 1 + x_j} \leq 1.$$

Prova. Seja $p(X) = (X + x_1) \ldots (X + x_n)$. Pelo problema 3, página 83, temos

$$\frac{p'(x)}{p(x)} = \sum_{i=1}^{n} \frac{1}{x + x_i}$$

para $x \neq -x_1, \ldots, -x_n$. Portanto, queremos mostrar que

$$\frac{p'(n-1)}{p(n-1)} \leq 1.$$

Para o que falta, para $1 \leq i \leq n$, seja $a_i = s_i(x_1, \ldots, x_n)$ a $i-$ésima soma simétrica elementar de $x_1, \ldots, x_n$, e faça $a_0 = 1$. Então, temos

$$p(X) = \sum_{j=0}^{n} a_j X^{n-j} \;\text{ e }\; p(X) = \sum_{j=0}^{n-1} (n-j) a_j X^{n-j-1},$$

de sorte que basta mostrar que

$$\sum_{j=0}^{n} a_j (n-1)^{n-j} \geq \sum_{j=0}^{n-1} (n-j) a_j (n-1)^{n-j-1}$$

ou, ainda,

$$\sum_{j=1}^{n-1} a_j (j-1)(n-1)^{n-j-1} + a_n \geq n a_0 (n-1)^{n-1} - a_0 (n-1)^n.$$

Finalmente, queremos provar que

$$\sum_{j=1}^{n} a_j (j-1)(n-1)^{n-j-1} \geq (n-1)^{n-1}.$$

Pela desigualdade entre as médias aritmética e geométrica, temos

$$a_j = \sum_{i_1 < \cdots < i_j} x_{i_1} \ldots x_{i_j} \geq \binom{n}{j} \sqrt[\binom{n}{j}]{\prod_{i_1 < \cdots < i_j} x_{i_1} \ldots x_{i_j}} = \binom{n}{j}.$$

de modo que basta mostrarmos que

$$\sum_{j=1}^{n} \binom{n}{j} (j-1)(n-1)^{n-j-1} \geq (n-1)^{n-1}.$$

Afirmamos que tal desigualdade é, de fato, uma igualdade. De fato, a igualdade

$$X^n = (X - 1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} (X-1)^{n-k}$$

nos dá, por derivação,

$$nX^{n-1} = \sum_{k=0}^{n-1} (n-k) \binom{n}{k} (X-1)^{n-k-1}.$$

Avaliando as funções polinomiais correspondentes em $x = n$, vem que

$$\begin{aligned}
n^n &= \sum_{k=0}^{n-1} (n-k) \binom{n}{k} (n-1)^{n-k-1} \\
&= \sum_{k=0}^{n-1} [(n-1) - (k-1)] \binom{n}{k} (n-1)^{n-k-1} \\
&= \sum_{k=0}^{n-1} \binom{n}{k} (n-1)^{n-k} - \sum_{k=0}^{n-1} (k-1) \binom{n}{k} (n-1)^{n-k-1}.
\end{aligned}$$

Por outro lado,

$$n^n = (n - 1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} (n-1)^{n-k},$$

de forma que

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n}{k} (n-1)^{n-k} &= \sum_{k=0}^{n-1} \binom{n}{k} (n-1)^{n-k} \\
&\quad - \sum_{k=0}^{n-1} (k-1) \binom{n}{k} (n-1)^{n-k-1}.
\end{aligned}$$

Após efetuar os cancelamentos óbvios, chegamos à igualdade

$$\binom{n}{n}(n-1)^{n-n}+\sum_{k=0}^{n-1}(k-1)\binom{n}{k}(n-1)^{n-k-1}=0$$

ou, ainda, a

$$\sum_{k=0}^{n}(k-1)\binom{n}{k}(n-1)^{n-k-1}=0.$$

Por fim, a partir daí, obtemos

$$(0-1)\binom{n}{0}(n-1)^{n-0-1}+\sum_{k=1}^{n}(k-1)\binom{n}{k}(n-1)^{n-k-1}=0,$$

que é precisamente a igualdade desejada. □

Problemas – Seção 4.2

1. Sejam f, g e h polinômios não nulos em $\mathbb{K}[X_1,\ldots,X_n]$, tais que f e g são simétricos e $f=gh$. Prove que h é simétrico.

2. * Um polinômio $f\in\mathbb{K}[X_1,\ldots,X_n]$ é denominado **homogêneo** de grau k quando

$$f(tX_1,\ldots,tX_n)=t^kf(X_1,\ldots,X_n),$$

para todo $t\in\mathbb{K}$. Obtenha, a menos de multiplicação por constantes, todos os polinômios simétricos e homogêneos de grau 2 em $\mathbb{R}[X,Y,Z]$.

3. Para $f\in\mathbb{K}[X_1,\ldots,X_n]$, seja $g\in\mathbb{K}[X_1,\ldots,X_n]$ o polinômio definido por

$$g(X_1,\ldots,X_n)=\frac{1}{n!}\sum_{\sigma}f(X_{\sigma(1)},\ldots,X_{\sigma(n)}),$$

onde σ varia sobre todas as $n!$ permutações de I_n. Prove que g é um polinômio simétrico, denominado a **simetrização** de f, e que $g=f$ se f for simétrico.

4. (Croácia.) Se a, b e c são reais dois a dois distintos satisfazendo o sistema de equações

$$\begin{cases} a^3=3b^2+3c^2-25 \\ b^3=3c^2+3a^2-25 \\ c^3=3a^2+3b^2-25 \end{cases},$$

calcule os possíveis valores do produto abc.

5. Dados $a,b,c\in\mathbb{C}$, explicite, em função de a, b e c, os coeficientes de um polinômio mônico de grau três cujas raízes complexas sejam os cubos das raízes complexas do polinômio X^3+aX^2+bX+c.

6. Dado o polinômio $p(x)=X^3-X^2+X+1$, pede-se:

   (a) Mostrar que p tem três raízes distintas, duas das quais são complexas e não reais.

   (b) Obter o polinômio mônico de terceiro grau cujas raízes são os cubos das raízes de p.

7. (OBM.) Sabendo que o polinômio $f(X)=X^3+pX+q$ tem três raízes reais distintas, prove que $p<0$.

8. (Romênia.) Sejam a, b e c complexos não nulos, tais que

$$a+b+c=\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=0.$$

Se n for um inteiro positivo, mostre que $a^n+b^n+c^n=0$ se, e só se, $3\nmid n$.

9. (Hong Kong.) Sejam $a_3, a_4, \ldots, a_{100}$ números reais, sendo $a_{100} \neq 0$. Prove que nem todas as raízes do polinômio

$$f(X) = a_{100}X^{100} + a_{99}X^{99} + \cdots + a_3X^3 + 3X^2 + 2X + 1$$

são reais.

10. Considere todas as retas que encontram o gráfico da função polinomial real $f(x) = 2x^4 + 7x^3 + 3x - 5$ em quatro pontos distintos (x_i, y_i), para $1 \leq i \leq 4$. Prove que o número $\frac{1}{4}(x_1 + x_2 + x_3 + x_4)$ independe da reta considerada e calcule seu valor.

11. (Moldávia.) No plano cartesiano, um círculo intersecta a hipérbole de equação $xy = 1$ em quatro pontos distintos. Prove que o produto das abscissas dos pontos de interseção é sempre igual a 1.

12. (Canadá - adaptado.) Sejam a, b e c as raízes complexas do polinômio $X^3 - X^2 - X - 1$.

    (a) Prove que a, b e c são duas a duas distintas.

    (b) Se, para cada $n \in \mathbb{N}$, pusermos

    $$S_n = \frac{a^n - b^n}{a - b} + \frac{b^n - c^n}{b - c} + \frac{c^n - a^n}{c - a},$$

    mostre que $S_{k+3} = S_{k+2} + S_{k+1} + S_k$, para todo $k \in \mathbb{N}$.

    (c) Conclua que $S_n \in \mathbb{Z}$, para todo $n \in \mathbb{N}$.

13. (BMO - adaptado.) Para números reais x e y tais que $xy \neq -1$, defina

    $$x * y = \frac{1 + x + y}{1 + xy}.$$

    (a) Dados $n \geq 2$ reais positivos $x_1, x_2, \ldots, x_n$, mostre que

    $$x_1 * (x_2 * (\cdots * x_n) \cdots) = \frac{s_1 + s_3 + \cdots + s_i}{1 + s_2 + s_4 + \cdots + s_p},$$

    onde i e p são, respectivamente, o maior ímpar e o maior par menores ou iguais a n e s_j é a j−ésima soma simétrica elementar de $x_1, x_2, \ldots, x_n$.

    (b) Se $f(X) = (X + x_1)(X + x_2) \ldots (X + x_n)$, use o resultado do item (a) para mostrar que

    $$x_1 * (x_2 * (\cdots * x_n) \cdots) = \frac{f(1) + (-1)^{n+1} f(-1)}{f(1) + (-1)^n f(-1)}.$$

14. Seja $n > 1$ inteiro. Obtenha todas as soluções reais do sistema

$$\begin{cases} x_1 + x_2 + \cdots + x_n = n \\ x_1^2 + x_2^2 + \cdots + x_n^2 = n \\ \cdots \\ x_1^n + x_2^n + \cdots + x_n^n = n \end{cases}.$$

15. Seja $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + 1$ um polinômio de coeficientes reais não negativos e raízes reais. Prove que $f(x) \geq (x + 1)^n$, para todo real $x \geq 0$.

16. (Irlanda.) Dado $n \in \mathbb{N}$, ache todos os polinômios $f(X) = a_nX^n + \cdots + a_1X + a_0$ satisfazendo as seguintes condições:

    (a) $a_j \in \{-1, 1\}$, para $0 \leq j \leq n$.

    (b) Todas as raízes de f são reais.

4.3 O teorema de Newton

Ainda sobre polinômios simétricos, note que $f(X, Y, Z) = X^4 + Y^4 + Z^4$ é simétrico mas não é um dos polinômios simétricos em X,

Y e Z que chamamos *elementares.* Contudo, sendo $s_1 = s_1(X, Y, Z)$, $s_2 = s_2(X, Y, Z)$ e $s_3 = s_3(X, Y, Z)$, podemos escrever

$$\begin{aligned} f(X,Y,Z) &= (X^2+Y^2+Z^2)^2 - 2(X^2Y^2+X^2Z^2+Y^2Z^2) \\ &= \left[(X+Y+Z)^2 - 2(XY+XZ+YZ)\right]^2 \\ &\quad - 2\left[(XY+XZ+YZ)^2 - 2XYZ(X+Y+Z)\right] \\ &= (s_1^2-2s_2)^2 - 2(s_2^2-2s_1s_3) \\ &= s_1^4 - 4s_1^2s_2 + 2s_2^2 + 4s_1s_3 \\ &= g(s_1,s_2,s_3), \end{aligned}$$

onde

$$g(X,Y,Z) = X^4 - 4X^2Y + 2Y^2 + 4XZ.$$

Assim, nesse caso particular, fomos capazes de expressar o polinômio simétrico $f(X, Y, Z) = X^4 + Y^4 + Z^4$ como um *polinômio nos polinômios simétricos elementares em X, Y e Z.*

Conforme veremos nesta seção, tal possibilidade não é acidental. Mais precisamente, provaremos a seguir um resultado usualmente atribuído ao matemático e físico inglês Isaac Newton, conhecido na literatura como o **teorema fundamental dos polinômios simétricos**.

No que segue, $\mathbb{K}$ inclui a possibilidade $\mathbb{K} = \mathbb{Z}$. Seguimos, essencialmente, a exposição de [27].

Teorema 4.12 (Newton). *Se $f = f(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$ é simétrico, então existe $g \in \mathbb{K}[X_1, \ldots, X_n]$ tal que*

$$f(X_1, \ldots, X_n) = g(s_1, \ldots, s_n),$$

onde $s_1, \ldots, s_n \in \mathbb{K}[X_1, \ldots, X_n]$ são os polinômios simétricos elementares em $X_1, \ldots, X_n$.

Para a prova do teorema anterior, precisamos introduzir alguns conceitos preliminares. Inicialmente, vamos *ordenar* os monômios

de $\mathbb{K}[X_1, \ldots, X_n]$ da seguinte maneira: dadas duas $n-$uplas distintas $(i_1, \ldots, i_n)$ e $(j_1, \ldots, j_n)$ de inteiros não negativos e monômios $a_{(i)}X_1^{i_1} \ldots X_n^{i_n}$ e $b_{(j)}X_1^{j_1} \ldots X_n^{j_n}$ em $\mathbb{K}[X_1, \ldots, X_n]$, definimos

$$\begin{gathered} a_{(i)}X_1^{i_1} \ldots X_n^{i_n} \prec b_{(j)}X_1^{j_1} \ldots X_n^{j_n} \\ \Updownarrow \\ \exists 1 \le k \le n; \begin{cases} i_l = j_l \text{ se } l < k \\ i_k < j_k \end{cases}. \end{gathered} \tag{4.4}$$

Neste caso, dizemos que $b_{(j)}X_1^{j_1} \ldots X_n^{j_n}$ é *maior do que* $a_{(i)}X_1^{i_1} \ldots X_n^{i_n}$.

Em geral, nos referiremos à ordenação acima como a **ordem lexicográfica** dos monômios de $\mathbb{K}[X_1, \ldots, X_n]$. Em particular, para $f \in \mathbb{K}[X_1, \ldots, X_n]$, seu *termo líder* é o monômio máximo (i.e., maior que todos os demais) em relação à ordem lexicográfica. Note ainda que, em $\mathbb{K}[X]$, tem-se $1 \prec X \prec X^2 \prec \cdots$, de modo que a noção de termo líder em mais de uma indeterminada generaliza a noção usual em uma indeterminada, dada pelo grau de um monômio.

Exemplo 4.13. *Se $f = s_1^{k_1} \ldots s_n^{k_n}$, onde $s_i \in \mathbb{K}[X_1, \ldots, X_n]$ é o $i-$ésimo polinômio simétrico elementar, então f tem termo líder*

$$X_1^{k_1+k_2+\cdots+k_n} X_2^{k_2+\cdots+k_n} \ldots X_{n-1}^{k_{n-1}+k_n} X_n^{k_n}.$$

De fato, uma vez que

$$f = \left(\sum_i X_i\right)^{k_1} \left(\sum_{i<j} X_iX_j\right)^{k_2} \ldots (X_1 \ldots X_n)^{k_n},$$

a definição de ordem lexicográfica garante que seu termo líder é

$$X_1^{k_1}(X_1X_2)^{k_2}(X_1X_2X_3)^{k_3} \ldots (X_1 \ldots X_n)^{k_n},$$

i.e.,

$$X_1^{k_1+k_2+\cdots+k_n} X_2^{k_2+\cdots+k_n} \ldots X_n^{k_n}.$$

De posse do conceito de ordem lexicográfica, a chave para a prova do teorema de Newton se encontra no seguinte resultado auxiliar.

Lema 4.14. *Se $f \in \mathbb{K}[X_1, \ldots, X_n]$ é simétrico e $a_{(\alpha)}X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ é seu termo líder, então*

$$\alpha_1 \geq \cdots \geq \alpha_n.$$

Prova. Se α_1 é o maior expoente que comparece em algum monômio de f, então, como f é simétrico, existe em f um monômio contendo $X_1^{\alpha_1}$. Se $a_{(i)}X_1^{i_1} \ldots X_n^{i_n}$ é um monômio de f tal que $i_1 < \alpha_1$, segue da definição da ordem lexicográfica que tal monômio não é o termo líder de f. Portanto, o termo líder contém $X_1^{\alpha_1}$.

Agora, dentre todos os monômios de f contendo $X_1^{\alpha_1}$, selecione um com expoente máximo em alguma das indeterminadas $X_2, \ldots, X_n$, digamos expoente α_2. Novamente por ser f simétrico, existe um tal monômio de f contendo $X_1^{\alpha_1}X_2^{\alpha_2}$. Ademais, pela escolha de α_1 temos $\alpha_1 \geq \alpha_2$. Por outro lado, se $a_{(i)}X_1^{\alpha_1}X_2^{i_2} \ldots X_n^{i_n}$ é monômio de f tal que $i_2 < \alpha_2$, então, novamente pela definição de ordem lexicográfica, tal monômio não é o termo líder de f, de modo que o termo líder de f contém $X_1^{\alpha_1}X_2^{\alpha_2}$. Por fim, repetindo esse argumento mais $n-2$ vezes, obtemos o resultado desejado. □

Podemos, finalmente, apresentar a prova do teorema de Newton.

Prova do teorema 4.12. Tome $f \in \mathbb{K}[X_1, \ldots, X_n]$ simétrico, com termo líder $a_{(\alpha)}X_1^{\alpha_1} \ldots X_n^{\alpha_n}$. Pelo lema anterior, temos $\alpha_1 \geq \cdots \geq \alpha_n$. Por outro lado, pelo exemplo 4.13, o polinômio simétrico

$$g(X_1, \ldots, X_n) = a_{(\alpha)}s_1^{\alpha_1-\alpha_2}s_2^{\alpha_2-\alpha_3} \ldots s_{n-1}^{\alpha_{n-1}-\alpha_n}s_n^{\alpha_n}$$

também tem termo líder $a_{(\alpha)}X_1^{\alpha_1} \ldots X_n^{\alpha_n}$, de modo que o polinômio simétrico $f-g$ tem termo líder $a_{(\beta)}X_1^{\beta_1} \ldots X_n^{\beta_n}$, com $a_{(\beta)}X_1^{\beta_1} \ldots X_n^{\beta_n} \prec a_{(\alpha)}X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ na ordem lexicográfica. Mas, como $\mathbb{K}[X_1, \ldots, X_n]$ contém somente um número finito de monômios mônicos e menores que $a_{(\alpha)}X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ em relação à ordem lexicográfica, um número finito de repetições do algoritmo acima nos dá $f-g = l(s_1, \ldots, s_n)$, para algum polinômio $l \in \mathbb{K}[X_1, \ldots, X_n]$. Assim, o mesmo ocorre com f. □

Vale frisar que o teorema de Newton é, primordialmente, um teorema de existência. De fato, é possível provar que, para polinômios simétricos em geral, o algoritmo descrito na prova do teorema de Newton não termina em tempo polinomial (i.e., mesmo com o auxílio de um computador não conseguimos, para um polinômio simétrico genérico em n indeterminadas, expressá-lo, em tempo finito, como um polinômio nos polinômios simétricos elementares em n indeterminadas). Todavia, mostraremos, no exemplo a seguir que a mera existência assegurada pelo teorema de Newton pode ser bastante útil. Para outra aplicação interessante, veja a seção 8.1.

Exemplo 4.15 (Miklós Schweitzer). *Seja $f \in \mathbb{Z}[X]$ um polinômio não constante e $\omega = \text{cis}\,\frac{2\pi}{n}$, onde $n > 1$ é um inteiro. Prove que*

$$f(\omega)f(\omega^2) \ldots f(\omega^{n-1}) \in \mathbb{Z}.$$

Prova. Considere o polinômio $g \in \mathbb{Z}[X_1, \ldots, X_{n-1}]$ dado por

$$g(X_1, \ldots, X_{n-1}) = f(X_1)f(X_2) \ldots f(X_{n-1}).$$

Se σ é uma permutação de I_{n-1}, então

$$\{\sigma(1), \sigma(2), \ldots, \sigma(n-1)\} = \{1, 2, \ldots, n-1\}$$

e, daí,

$$\begin{aligned} g(X_{\sigma(1)}, \ldots, X_{\sigma(n-1)}) &= f(X_{\sigma(1)})f(X_{\sigma(2)}) \ldots f(X_{\sigma(n-1)}) \\ &= f(X_1)f(X_2) \ldots f(X_{n-1}) \\ &= g(X_1, \ldots, X_{n-1}). \end{aligned}$$

Assim, g é simétrico e o teorema de Newton garante a existência de um polinômio $h \in \mathbb{Z}[X_1, \ldots, X_{n-1}]$ tal que $g(X_1, \ldots, X_{n-1}) = h(s_1, \ldots, s_{n-1})$, i.e.,

$$f(X_1)f(X_2)\ldots f(X_{n-1}) = h(s_1, \ldots, s_{n-1}),$$

onde s_j é o j-ésimo polinômio simétrico elementar em $X_1, \ldots, X_{n-1}$.

Substituindo X_j por ω^j na igualdade acima, obtemos

$$f(\omega)f(\omega^2)\ldots f(\omega^{n-1}) = h(s_1(\omega, \ldots, \omega^{n-1}), \ldots, s_{n-1}(\omega, \ldots, \omega^{n-1}));$$

portanto, a fim de mostrar que $f(\omega)f(\omega^2)\ldots f(\omega^{n-1}) \in \mathbb{Z}$, é suficiente mostrar que $s_j(\omega, \ldots, \omega^{n-1}) \in \mathbb{Z}$, para $1 \leq j \leq n-1$.

Para o que falta, basta observar que

$$\begin{aligned} X^n - 1 &= (X-1)(X-\omega)(X-\omega^2)\ldots(X-\omega^{n-1}) \\ &= (X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1), \end{aligned}$$

de sorte que

$$\begin{aligned} X^{n-1} + X^{n-2} + \cdots + X + 1 &= (X-\omega)(X-\omega^2)\ldots(X-\omega^{n-1}) \\ &= \sum_{j=0}^{n-1}(-1)^j s_j(\omega, \omega^2, \ldots, \omega^{n-1})X^{n-1-j}. \end{aligned}$$

Assim, temos que

$$s_j(\omega, \omega^2, \ldots, \omega^{n-1}) = (-1)^j \in \mathbb{Z},$$

conforme desejado. □

A discussão que antecede o exemplo anterior sugere que, quando quisermos expressar *efetivamente* um dado polinômio simétrico como um polinômio nos polinômios simétricos elementares, teremos, via de regra, de recorrer a argumentos *ad hoc*. Nesse sentido, terminamos esta seção discutindo um exemplo relevante, para o qual precisamos da seguinte consequência do algoritmo de Horner-Rufinni. As identidades (4.5) a seguir são conhecidas como as **identidades de Horner-Ruffini**.

Lema 4.16 (Horner-Rufinni). *Seja*

$$f(X) = X^n - s_1X^{n-1} + \cdots + (-1)^{n-1}s_{n-1}X + (-1)^n s_n$$

um polinômio não constante sobre $\mathbb{C}$. *Se* z *é uma raiz complexa de* f *e*

$$g(X) = X^{n-1} + b_1X^{n-2} + \cdots + b_{n-1}$$

é o quociente da divisão de $f(X)$ *por* $X - z$, *então*

$$\left\{\begin{array}{lcl} b_1 &=& z - s_1 \\ b_2 &=& z^2 - s_1z + s_2 \\ \cdots && \cdots \\ b_{k+1} &=& z^{k+1} - s_1z^k + \cdots + (-1)^{k+1}s_{k+1} \\ \cdots && \cdots \\ b_{n-1} &=& z^{n-1} - s_1z^{n-2} + \cdots + (-1)^{n-1}s_{n-1} \end{array}\right. . \tag{4.5}$$

Prova. Nas notações do enunciado, as recorrências (3.1) se escrevem

$$\left\{\begin{array}{lcl} b_1 &=& z - s_1 \\ b_2 &=& zb_1 + s_2 \\ \cdots && \cdots \\ b_{k+1} &=& zb_k + (-1)^{k+1}s_{k+1} \\ \cdots && \cdots \\ b_{n-1} &=& zb_{n-2} + (-1)^{n-1}s_{n-1} \end{array}\right. .$$

Resolvendo o sistema linear acima sucessivamente para $b_2, \ldots, b_{n-1}$, obtemos uma a uma as relações do enunciado. □

As relações contidas na proposição a seguir nos fornecerão recorrências para expressar o polinômio simétrico

$$\sigma_k(X_1, X_2, \ldots, X_n) = X_1^k + X_2^k + \cdots + X_n^k$$

como um polinômio nos polinômios simétricos elementares em $X_1, X_2, \ldots, X_n$. As fórmulas dos itens (a) e (b) a seguir são respectivamente

denominadas primeira e segunda **identidades de Jacobi**[2]. Para uma outra prova das mesmas, veja o problema 2, página 242.

Proposição 4.17 (Jacobi). *Para* $z_1, \ldots, z_n \in \mathbb{C}$, *se* $s_i = s_i(z_1, \ldots, z_n)$ *é a* $i-$*ésima soma simétrica elementar de* $z_1, \ldots, z_n$ *e* $\sigma_k = z_1^k + \cdots + z_n^k$, *então:*

(a) $\sigma_{n+k} = \sum_{j=1}^{n}(-1)^{j-1}s_j\sigma_{n+k-j}$, *para* $k \geq 1$.

(b) $s_{k+1} = \frac{1}{k+1}\sum_{j=1}^{k+1}(-1)^{j-1}s_{k+1-j}\sigma_j$, *para* $1 \leq k \leq n-1$.

Prova.
(a) Seja

$$f(X) = (X - z_1)\ldots(X - z_n) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n. \quad (4.6)$$

Como z_i é raiz de f, temos

$$z_i^n - s_1 z_i^{n-1} + \cdots + (-1)^{n-1}s_{n-1}z_i + (-1)^n s_n = 0$$

para $1 \leq i \leq n$ e, daí,

$$z_i^{k+n} - s_1 z_i^{k+n-1} + \cdots + (-1)^{n-1}s_{n-1}z_i^{k+1} + (-1)^n s_n z_i^k = 0.$$

Somando as igualdades acima para $1 \leq i \leq n$, obtemos

$$\sigma_{n+k} - s_1\sigma_{n+k-1} + \cdots + (-1)^{n-1}s_{n-1}\sigma_{k+1} + (-1)^n s_n\sigma_k = 0,$$

igualdade equivalente à do enunciado.

(b) Segue de (4.6) que

$$f'(X) = nX^{n-1} - (n-1)s_1X^{n-2} + \cdots + (-1)^{n-1}s_{n-1}. \quad (4.7)$$

[2]Após o matemático alemão do século XIX Carl G. J. Jacobi.

Por outro lado, para $z \in \mathbb{C} \setminus \{z_1, \ldots, z_n\}$, segue do problema 3, página 83, que

$$f'(z) = \frac{f(z)}{z - z_1} + \cdots + \frac{f(z)}{z - z_n}.$$

Sendo $f_j \in \mathbb{C}[X]$ tal que $f(X) = (X - z_j)f_j(X)$, digamos

$$f_j(X) = X^{n-1} + b_{1j}X^{n-2} + \cdots + b_{n-1,j},$$

segue que

$$\begin{aligned} f'(z) &= \sum_{j=1}^{n} f_j(z) = \sum_{j=1}^{n}(z^{n-1} + b_{1j}z^{n-2} + \cdots + b_{n-1,j}) \\ &= nz^{n-1} + \left(\sum_{j=1}^{n} b_{1j}\right)z^{n-2} + \cdots + \left(\sum_{j=1}^{n} b_{n-1,j}\right). \end{aligned}$$

Mas, como a igualdade acima é válida para todo $z \in \mathbb{C} \setminus \{z_1, \ldots, z_n\}$, segue do corolário 3.10 que

$$f'(X) = nX^{n-1} + \left(\sum_{j=1}^{n} b_{1j}\right)X^{n-2} + \cdots + \left(\sum_{j=1}^{n} b_{n-1,j}\right). \quad (4.8)$$

Por fim, igualando os coeficientes correspondentes em (4.7) e (4.8) e substituindo as identidades (4.5), obtemos

$$\begin{aligned} (-1)^{k+1}(n-k-1)s_{k+1} &= \sum_{j=1}^{n} b_{k+1,j} \\ &= \sum_{j=1}^{n}(z_j^{k+1} - s_1 z_j^k + \cdots + (-1)^{k+1}s_{k+1}) \\ &= \sigma_{k+1} - s_1\sigma_k + \cdots + (-1)^{k+1}ns_{k+1}, \end{aligned}$$

de maneira que

$$(k+1)s_{k+1} = s_k\sigma_1 - s_{k-1}\sigma_2 + \cdots + (-1)^k s_0\sigma_{k+1}.$$

□

O corolário a seguir também é devido a Jacobi.

Corolário 4.18 (Jacobi). *Para cada inteiro $k \geq 1$, sejam s_k o k–ésimo polinômio simétrico elementar em $X_1, \ldots, X_n$ e $\sigma_k = X_1^k + \cdots + X_n^k$. Então:*

(a) $\sigma_{n+k} = \sum_{j=1}^{n} (-1)^{j-1} s_j \sigma_{n+k-j}$, *para* $k \geq 1$.

(b) $s_{k+1} = \frac{1}{k+1} \sum_{j=1}^{k+1} (-1)^{j-1} s_{k+1-j} \sigma_j$, *para* $1 \leq k \leq n-1$.

Prova. Avaliando ambos os membros de (a) e (b) em $z_1, \ldots, z_n \in \mathbb{C}$ obtemos, pela proposição anterior, igualdades verdadeiras. Como $\mathbb{C}$ é um conjunto infinito, a proposição 4.1 garante a igualdade dos polinômios correspondentes. □

Problemas – Seção 4.3

1. Se $f \in \mathbb{Z}[X]$ é um polinômio mônico, de grau $n \geq 1$ e raízes complexas $z_1, \ldots, z_n$, prove que $z_1^k + \cdots + z_n^k \in \mathbb{Z}$, para todo $k \geq 1$ inteiro.

2. Se $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ são números complexos tais que
$$a_1^k + \cdots + a_n^k = b_1^k + \cdots + b_n^k,$$
para $1 \leq k \leq n$, mostre que $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_n\}$.

3. (Japão - adaptado.) Sejam $n, k \in \mathbb{N}$, com $2 \leq k \leq n$, e $a_1, \ldots, a_k$ números reais tais que
$$\begin{cases} a_1 + \cdots + a_k &= n \\ a_1^2 + \cdots + a_k^2 &= n \\ \quad\cdots & \\ a_1^k + \cdots + a_k^k &= n \end{cases}.$$
Se $p(X) = (X+a_1)\ldots(X+a_k)$, prove que $p(X) = \sum_{j=0}^{k} \binom{n}{j} X^{k-j}$.

4. Sejam $m \in \mathbb{N}$, $\omega = \cos\frac{2\pi}{m} + i \operatorname{sen}\frac{2\pi}{m}$ e $z_1, \ldots, z_n$ números complexos tais que
$$f(X) = (X - z_1)(X - z_2)\ldots(X - z_n)$$
é um polinômio de coeficientes inteiros.
   (a) Se $g(X) = \prod_{i=0}^{m-1} f(\omega^i X)$, prove que
   $$g(X) = (X^m - z_1^m)\ldots(X^m - z_n^m).$$
   (b) Use as identidades de Jacobi para mostrar que o polinômio g do item (a) tem coeficientes inteiros.
   (c) Conclua que, se $z \in \mathbb{C}$ é raiz de um polinômio não nulo f de coeficientes inteiros, então existe um polinômio não nulo h, também de coeficientes inteiros, tal que z^m é raiz de h.

5. (OBM.)
   (a) Se $n \in \mathbb{N}$, prove que há somente um número finito de polinômios mônicos, de grau n e coeficientes inteiros, tais que todas as suas raízes complexas têm módulo 1.
   (b) Seja $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ um polinômio mônico, tal que todas as suas raízes complexas têm módulo 1. Prove que todas as raízes complexas de f são raízes da unidade.

CAPÍTULO 5

Polinômios sobre $\mathbb{R}$

Neste capítulo, revisitamos alguns dos teoremas clássicos do Cálculo, estudados em [12], para polinômios de coeficientes reais, tendo como ferramenta principal o teorema fundamental da álgebra. Como aplicação dos mesmos, provaremos as desigualdades de Newton, as quais generalizam a desigualdade entre as médias aritmética e geométrica de n números reais positivos, e a regra de Descartes, que relaciona o número de raízes positivas de um polinômio de coeficientes reais ao número de trocas de sinal de seus coeficientes não nulos.

5.1 Alguns teoremas do Cálculo

Nosso primeiro resultado dá uma condição suficiente para a existência de raízes reais num intervalo. Para a prova do mesmo, precisamos do seguinte resultado auxiliar.

Lema 5.1. *Se $f \in \mathbb{R}[X] \setminus \{0\}$ é mônico e não tem raízes reais, então existem polinômios $g, h \in \mathbb{R}[X]$ tais que $f = g^2 + h^2$. Em particular, $f(x) > 0$ para todo $x \in \mathbb{R}$.*

Prova. Pelo problema 2, página 74, existem números complexos não reais $z_1, \ldots, z_k$ tais que

$$f(X) = \prod_{j=1}^{k}(X - z_j)(X - \overline{z}_j).$$

Agora, se $z_j = a_j + ib_j$, com $a_j, b_j \in \mathbb{R}$, então

$$\begin{aligned}(X - z_j)(X - \overline{z}_j) &= (X - a_j - ib_j)(X - a_j + ib_j)\\ &= (X - a_j)^2 - (ib_j)^2\\ &= (X - a_j)^2 + b_j^2,\end{aligned}$$

a soma dos quadrados de dois polinômios de coeficientes reais (um deles constante).

Basta, agora, aplicar várias vezes um argumento similar à identidade de Euler (7.7) de [14]: para $g_1, g_2, h_1, h_2 \in \mathbb{R}[X]$, temos

$$(g_1^2 + h_1^2)(g_2^2 + h_2^2) = (g_1g_2 + h_1h_2)^2 + (g_1h_2 - g_2h_1)^2.$$

Para o que falta, segue da primeira parte que

$$f(x) = g(x)^2 + h(x)^2 \geq 0,$$

para todo $x \in \mathbb{R}$; mas, como f não tem raízes reais, a desigualdade acima deve ser estrita, para todo $x \in \mathbb{R}$. □

O resultado a seguir é o teorema do valor intermediário para polinômios, sendo conhecido na literatura como o **teorema de Bolzano**[1].

[1] Após Bernhard Bolzano, matemático alemão do século XIX.

Teorema 5.2 (Bolzano). *Se $f \in \mathbb{R}[X]$ e $a < b$ são reais tais que $f(a)f(b) < 0$, então existe $c \in (a, b)$ tal que $f(c) = 0$.*

Prova. Supondo, sem perda de generalidade, que f é mônico e $f(a) < 0 < f(b)$, segue da última parte do lema anterior que f tem ao menos uma raiz real. Sejam, pois, $a_1 \leq \cdots \leq a_k$ as raízes reais de f, repetidas de acordo com suas multiplicidades. Se $g \in \mathbb{R}[X]$ é tal que

$$f(X) = g(X)(X - a_1) \ldots (X - a_k),$$

então g é mônico e não possui raízes reais, de sorte que, novamente pelo lema anterior, $g(x) > 0$ para todo $x \in \mathbb{R}$.

Por contradição, suponha que não há raiz de f no intervalo (a, b) e considere três casos separadamente:

(i.) $a_k < a$: temos

$$f(a) = g(a)(a - a_1) \ldots (a - a_k) > 0,$$

uma contradição.

(ii.) $b < a_1$: segue de $f(b) > 0$ que

$$g(b)(b - a_1) \ldots (b - a_k) > 0$$

e, daí, k é par (uma vez que $g(b) > 0$ e $b - a_i < 0$, para $1 \leq i \leq k$). Por outro lado, segue de $f(a) < 0$ que

$$g(a)(a - a_1) \ldots (a - a_k) < 0$$

e, daí, k é ímpar (uma vez que $g(a) > 0$ e $a - a_i < 0$, para $1 \leq i \leq k$). Portanto, chegamos a uma contradição.

(iii.) $a_l < a < b < a_{l+1}$, para algum $1 \leq l < k$: chegamos a um absurdo de modo análogo ao item anterior. (Por exemplo,

$$0 < f(a) = \underbrace{g(a)}_{>0}\underbrace{(a-a_1)\dots(a-a_l)}_{>0}\underbrace{(a-a_{l+1})\dots(a-a_k)}_{<0}$$

implica $k - l$ par.)

□

Exemplo 5.3 (Moldávia). *Sejam $f, g \in \mathbb{R}[X]$, cada um dos quais possuindo ao menos uma raiz real.*

(a) Prove que existe $a \in \mathbb{R}$ tal que $f(a)^2 = g(a)^2$.

(b) Se $f(1 + X + g(X)^2) = g(1 + X + f(X)^2)$, mostre que $f = g$.

Prova.
(a) Sejam α e β raízes de f e g, respectivamente. Podemos supor, sem perda de generalidade, que $\alpha \leq \beta$. Se $g(\alpha) = 0$ ou $f(\beta) = 0$, nada há a fazer. Senão, temos

$$f(\alpha)^2 - g(\alpha)^2 = -g(\alpha)^2 < 0 \text{ e } f(\beta)^2 - g(\beta)^2 = f(\beta)^2 > 0,$$

de sorte que o teorema de Bolzano, aplicado ao polinômio $f(X)^2 - g(X)^2$, garante a existência de $a \in (\alpha, \beta)$ tal que $f(a)^2 - g(a)^2 = 0$.

(b) Sendo $a \in \mathbb{R}$ como no item (a), defina uma sequência $(u_n)_{n\geq 1}$ pondo $u_0 = a$ e, para cada $n \geq 1$, $u_{n+1} = 1 + u_n + g(u_n)^2$. Pelo item (a), temos $f(u_1) = g(u_1)$. Suponha, por hipótese de indução, que $f(u_k) = g(u_k)$, para um certo inteiro $k \geq 1$. Então, nossas hipóteses garantem que

$$\begin{aligned} f(u_{k+1}) &= f(1 + u_k + g(u_k)^2) \\ &= g(1 + u_k + f(u_k)^2) \\ &= g(1 + u_k + g(u_k)^2) \\ &= g(u_{k+1}). \end{aligned}$$

Assim, temos $f(u_n) = g(u_n)$ para todo inteiro $n \geq 1$. Mas, como

$$u_{n+1} = 1 + u_n + g(u_n)^2 \geq 1 + u_n > u_n$$

para todo $n \geq 1$, segue do corolário 3.10 que $f = g$. □

No que segue, estabelecemos para polinômios o **teorema do valor médio** de Lagrange[2].

Teorema 5.4 (Lagrange). *Sejam $f \in \mathbb{R}[X] \setminus \{0\}$ e $a < b$ reais dados. Então existe $a < c < b$ tal que*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Prova. Provemos primeiro que, se $f(a) = f(b) = 0$, então existe $a < c < b$ tal que $f'(c) = 0$. Podemos supor, sem perda de generalidade, que f não tem outras raízes no intervalo (a, b). De fato, se f possuir uma infinidade de raízes em (a, b), temos $f = 0$, pelo corolário 3.9; se f possuir um número finito de raízes em (a, b), digamos $a_1 < a_2 < \cdots < a_k$, trocamos b por a_1.

Se existissem $a < c < d < b$ tais que $f(c)f(d) < 0$, o teorema de Bolzano garantiria a existência de uma raiz de f no intervalo (a, b), o que é um absurdo. Portanto, f tem sinal constante em (a, b). Suponha, sem perda de generalidade, que $f(x) > 0$ para $x \in (a, b)$, e sejam respectivamente k e l as multiplicidades de a e b como raízes de f. Então, existe $g \in \mathbb{R}[X]$ tal que

$$f(X) = (X - a)^k (X - b)^l g(X),$$

com $g(a), g(b) \neq 0$. Agora,

$$a < c < b \Rightarrow f(c) > 0 \Rightarrow (c - a)^k (c - b)^l g(c) > 0 \Rightarrow (-1)^l g(c) > 0.$$

[2]Após Joseph Louis Lagrange, matemático franco-italiano do século XVIII.

Consideremos o caso em que l é par (o caso em que l é ímpar é análogo), de sorte que $g(c) > 0$, para todo $c \in (a, b)$. Se $g(a) < 0$, o teorema de Bolzano garantiria a existência de $a < d < \frac{a+b}{2}$ tal que $g(d) = 0$, de modo que $f(d) = 0$, o que, por sua vez, é um absurdo. Logo, $g(a) > 0$ e, analogamente, $g(b) > 0$. Então, temos

$$\begin{aligned} f'(X) &= k(X-a)^{k-1}(X-b)^l g(X) + l(X-a)^k(X-b)^{l-1}g(X) \\ &\quad + (X-a)^k(X-b)^l g'(X) \\ &= (X-a)^{k-1}(X-b)^{l-1}h(X), \end{aligned}$$

onde

$$h(X) = (k(X-b) + l(X-a))g(X) + (X-a)(X-b)g'(X).$$

Basta, pois, então mostrarmos que existe $c \in (a, b)$ tal que $h(c) = 0$. Mas, como

$$h(a)h(b) = -kl(a-b)^2 g(a)g(b) < 0,$$

o teorema de Bolzano liquida a questão.

Para o caso geral, seja

$$f_1(X) = f(X) - f(a) - \left(\frac{f(b)-f(a)}{b-a}\right)(X-a).$$

Como $f_1(a) = f_1(b) = 0$, o que fizemos acima garante a existência de $c \in (a, b)$ tal que $f_1'(c) = 0$. Por fim, resta observar que

$$f_1'(X) = f'(X) - \left(\frac{f(b)-f(a)}{b-a}\right).$$

□

Conforme frisamos em [12], o caso $f(a) = f(b) = 0$ do teorema anterior precedeu a versão geral de Lagrange, tendo sido provado pelo matemático francês do século XVII Michel Rôlle e sendo conhecido na literatura como o **teorema de Rôlle**.

Corolário 5.5 (Rôlle). *Se $f \in \mathbb{R}[X] \setminus \{0\}$ e $a < b$ são reais tais que $f(a) = f(b) = 0$, então existe $a < c < b$ tal que $f'(c) = 0$.*

Ilustramos a utilização do teorema de Rôlle no exemplo a seguir.

Exemplo 5.6. *Seja $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n$ um polinômio de coeficientes reais, tal que*

$$\frac{a_0}{1} + \frac{a_1}{2} + \cdots + \frac{a_{n-1}}{n} + \frac{a_n}{n+1} = 0.$$

Prove que f possui pelo menos uma raiz no intervalo $(0, 1)$.

Prova. É imediato que $f = g'$, onde

$$g(X) = a_0X + \frac{a_1}{2}X^2 + \cdots + \frac{a_{n-1}}{n}X^n + \frac{a_n}{n+1}X^{n+1}.$$

Mas, como $g(0) = g(1) = 0$, o teorema de Rôlle garante a existência de $a \in (0, 1)$ tal que $f(a) = g'(a) = 0$. □

Uma consequência importante do teorema do valor médio é o estudo da primeira variação (i.e., crescimento ou decrescimento) de polinômios, conforme ensina o corolário a seguir.

Corolário 5.7. *Sejam $f \in \mathbb{R}[X] \setminus \{0\}$ e $I \subset \mathbb{R}$ um intervalo.*

(a) Se $f'(x) > 0$ para todo $x \in I$, então f é crescente em I.

(b) Se $f'(x) < 0$ para todo $x \in I$, então f é decrescente em I.

Prova. Façamos a prova do item (a), sendo a prova do item (b) análoga. Para $a < b$ em I, o teorema do valor médio garante a existência de $c \in (a, b)$ (e, portanto, $c \in I$) tal que

$$\frac{f(b)-f(a)}{b-a} = f'(c) > 0.$$

Em particular, $f(b) > f(a)$. □

Exemplo 5.8. *Prove que, para todo inteiro positivo n, o polinômio*

$$1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$$

tem no máximo uma raiz real.

Prova. Sendo $f_n = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$, mostremos que (i) f_n não tem raízes reais se n é par, e (ii) f_n tem exatamente uma raiz real se n é ímpar.

(i) Supondo n par, temos $\lim_{|x|\to+\infty} f_n(x) = +\infty$. Portanto, segue do teorema de Weierstrass (o teorema 4.31 de [12]) a existência de $x_0 \in \mathbb{R}$ tal que f_n assume seu valor mínimo em x_0. Suponha, por contradição, que $f_n(x_0) \leq 0$. Então, pelo resultado do problema 3, temos $f_n'(x_0) = 0$ e, como $f_n(x_0) = f_n'(x_0) + \frac{x_0^n}{n!}$, segue que $0 \geq f_n(x_0) = \frac{x_0^n}{n!}$. Como n é par, a única maneira de não termos uma contradição a partir dessa última relação é que seja $0 = f_n(x_0) = \frac{x_0^n}{n!}$. Mas aí, deveria ser $f_n(0) = 0$, o que é um absurdo.

(ii) Supondo n ímpar, segue do problema 4, página 75, que f_n tem um número ímpar de raízes reais; por outro lado, segue do exemplo 3.33 que f_n não tem raízes múltiplas. Suponha, então, que f_n tem pelo menos três raízes reais distintas, digamos $a < b < c$. Então, o teorema do valor médio garante a existência de $\alpha \in (a, b)$ e $\beta \in (b, c)$ tais que $f_n'(\alpha) = f_n'(\beta) = 0$. Mas, como $f_n' = f_{n-1}$ e $n-1$ é par, o caso anterior nos fornece uma contradição. □

Problemas – Seção 5.1

1. Se $f \in \mathbb{Z}[X]$ é um polinômio não constante e m é um inteiro positivo tal que $m > 1 + \text{Re}(z)$, para toda raiz complexa z de f, prove que $|f(m)| > 1$.

2. * Prove, para polinômios de coeficientes reais e com os métodos desta seção, o **teorema de permanência do sinal**: se $f \in \mathbb{R}[X]$ é tal que $f(a) > 0$ para algum $a \in \mathbb{R}$, então existe $r > 0$ tal que $f(x) > 0$ para todo $x \in (a - r, a + r)$.

3. * Dado $f \in \mathbb{R}[X] \setminus \mathbb{R}$, sejam $a \in \mathbb{R}$ e $r > 0$ tais que

$$f(a) = \min\{f(x);\ x \in (a - r, a + r)\}.$$

Prove que $f'(a) = 0$.

4. Seja $f(X) = X^5 - 2X^4 + 2$. Prove que f possui exatamente três raízes reais.

5. * Dado $f \in \mathbb{R}[X] \setminus \mathbb{R}$ com coeficiente líder positivo, prove que existe $n_0 \in \mathbb{N}$ tal que

$$u > v > n_0 \Rightarrow f(u) > f(v) > 0.$$

6. Prove que não existe polinômio $f \in \mathbb{Z}[X]$, tal que $f(n)$ seja primo para todo inteiro não negativo n.

7. (Leningrado[3].) Decida se existem quatro números reais distintos a, b, c e d tais que, para quaisquer dois deles, x e y digamos, tenhamos

$$x^{10} + x^9y + \cdots + xy^9 + y^{10} = 1.$$

8. Os reais positivos a_1, a_2, a_3 e a_4 são tais que $a_1 \leq a_2 \leq a_3 \leq a_4$ e $a_1a_2a_3a_4 = 1$. Se λ é uma raiz real do polinômio

$$X^3 - \left(\sum_{i=1}^4 a_i\right)X^2 + \left(\sum_{1\leq i<j\leq 4} a_ia_j\right)X - \left(\sum_{i=1}^4 \frac{1}{a_i}\right),$$

prove que $\lambda > a_2$.

[3] A cidade russa de São Petesburgo mudou seu nome para Leningrado durante a existência da União Soviética.

9. (Leningrado.) Sejam a, b, c, d e e números reais tais que o polinômio $aX^2 + (c-b)X + (e-d) = 0$ tem uma raiz real maior que 1. Prove que o polinômio $aX^4 + bX^3 + cX^2 + dX + e = 0$ tem ao menos uma raiz real.

10. (Áustria-Polônia.) Dados números reais $a_1, \ldots, a_n$, prove que

$$\sum_{i,j=1}^{n} \frac{a_i a_j}{i+j} \geq 0,$$

com igualdade se, e só se, $a_1 = \cdots = a_n = 0$.

11. Seja $f(X) = X^3 - 3X + 1$. Calcule o número de raízes reais distintas do polinômio $f(f(X))$.

12. (Suécia.) Seja $f \in \mathbb{R}[X]$ um polinômio de grau n. Se $f(x) \geq 0$ para todo $x \in \mathbb{R}$, mostre que

$$f(x) + f'(x) + f''(x) + \cdots + f^{(n)}(x) \geq 0,$$

para todo $x \in \mathbb{R}$.

13. Dois matemáticos A e B disputam o seguinte jogo: é dado um polinômio de grau par maior ou igual a 4,

$$f(X) = X^{2n} + a_{2n-1}X^{2n-1} + \cdots + a_1 X + 1,$$

onde $a_1, \ldots, a_{2n-1}$ são números reais não especificados. Os jogadores, começando por A, alternam-se especificando os coeficientes de f, até que f esteja completamente determinado. No final, A ganha se nenhuma raiz de f for real e B ganha caso contrário. Encontre uma estratégia ganhadora para B.

14. No começo de uma aula, o professor escreveu no quadro negro um polinômio de grau 3. A partir daí, os alunos, um por vez, vinham ao quadro e perfaziam uma das seguintes operações com o polinômio deixado pelo aluno anterior:

   (a) Adicionavam ao polinômio sua derivada.

   (b) Subtraíam do polinômio sua derivada.

   Ao final da aula, o polinômio inicial apareceu novamente no quadro negro. Prove que ao menos um dos alunos cometeu um erro.

15. (OIM.) São dados números reais a_1, a_2, $\ldots$, a_n, tais que $0 < a_1 < a_2 < \cdots < a_n$. Se $f : \mathbb{R} \setminus \{-a_1, \ldots, -a_n\} \to \mathbb{R}$ é a função tal que

$$f(x) = \sum_{j=1}^{n} \frac{a_j}{x + a_j},$$

para $x \neq -a_1, \ldots, -a_n$, prove que o conjunto $\{x \in \mathbb{R};\ f(x) \geq 1\}$ pode ser escrito como a união de n intervalos limitados, dois a dois disjuntos e cuja soma de comprimentos é igual a $a_1 + a_2 + \cdots + a_n$.

5.2 As desigualdades de Newton

Nesta seção, apresentamos um conjunto de desigualdades que refina a desigualdade entre as médias aritmética e geométrica (provada na seção 7.2 de [10]). Para tanto, precisamos inicialmente do resultado auxiliar a seguir.

Lema 5.9. *Se $f \in \mathbb{R}[X] \setminus \{0\}$ tem k raízes reais, então f' tem pelo menos $k-1$ raízes reais. Em particular, se todas as raízes de f forem reais, então todas as raízes de f' também serão reais.*

Prova. Podemos supor $k > 1$. Sejam $a_1 < \cdots < a_l$ as raízes reais distintas de f, com multiplicidades respectivamente iguais a $m_1, \ldots, m_l$, de tal modo que $m_1 + \cdots + m_l = k$. Então, já vimos na proposição 3.31 que cada a_i é raiz de multiplicidade $m_i - 1$ de f'. Por outro lado,

pelo teorema de Rôlle, entre a_i e a_{i+1} há pelo menos mais uma raiz real de f', de modo que contabilizamos ao menos

$$(m_1-1)+\cdots+(m_l-1)+(l-1)=k-1$$

raízes reais para f'. O resto é imediato. □

Para o que segue, dados $n>1$ reais positivos $a_1,a_2,\ldots,a_n$ e $0\leq i\leq n$, denotaremos simplesmente por $S_i(a_j)$ a i–ésima soma simétrica elementar de $a_1,\ldots,a_n$ e por $H_i(a_j)$ a média aritmética das $\binom{n}{i}$ parcelas que compõem $S_i(a_j)$, i.e.,

$$H_i(a_j)=\binom{n}{i}^{-1}S_i(a_j).$$

O teorema a seguir é frequentemente creditado a Isaac Newton.

Teorema 5.10. *Nas notações acima, para* $1\leq i<n$ *temos*

$$H_i(a_j)^2\geq H_{i-1}(a_j)H_{i+1}(a_j),$$

ocorrendo a igualdade para algum i *se, e só se,* $a_1=a_2=\cdots=a_n$.

Prova. Façamos indução sobre o número $n>1$ de reais positivos. Para $n=2$, queremos mostrar que $H_1^2(a_1,a_2)\geq H_0(a_1,a_2)H_2(a_1,a_2)$ ou, ainda, que

$$\left(\frac{a_1+a_2}{2}\right)^2\geq a_1a_2.$$

Mas isto é apenas a desigualdade entre as médias aritmética e geométrica, na qual a igualdade ocorre se e só se $a_1=a_2$.

Suponha, por hipótese de indução, que as desigualdades de Newton são válidas para $n-1$ reais positivos quaisquer, ocorrendo a igualdade em uma qualquer delas se e só se os $n-1$ números forem todos iguais.

Agora, consideremos $n\geq 3$ reais positivos $a_1,a_2,\ldots,a_n$, e seja

$$f(X)=(X+a_1)\ldots(X+a_n).$$

O lema anterior garante a existência de $n-1$ reais positivos $b_1,\ldots,b_{n-1}$ tais que

$$f'(X)=n(X+b_1)\ldots(X+b_{n-1}),$$

de modo que

$$\frac{1}{n}f'(X)=X^{n-1}+\binom{n-1}{1}H_1(b_j)X^{n-2}+\cdots+\binom{n-1}{n-1}H_{n-1}(b_j).$$

Por outro lado, $f(X)=\sum_{i=0}^{n}\binom{n}{i}H_i(a_j)X^{n-i}$ fornece

$$\begin{aligned}f'(X)&=\sum_{i=0}^{n-1}(n-i)\binom{n}{i}H_i(a_j)X^{n-i-1}\\&=n\sum_{i=0}^{n-1}\binom{n-1}{i}H_i(a_j)X^{n-1-i}\end{aligned}$$

e segue, daí, que

$$H_i(a_1,\ldots,a_n)=H_i(b_1,\ldots,b_{n-1}),$$

para $0\leq i\leq n-1$. Pela hipótese de indução, para $1\leq i\leq n-2$ temos

$$H_i^2(a_j)=H_i^2(b_j)\geq H_{i-1}^2(b_j)H_{i+1}^2(b_j)=H_{i-1}^2(a_j)H_{i+1}^2(a_j).\quad(5.1)$$

Resta somente provar que $H_{n-1}^2(a_j)\geq H_{n-2}(a_j)H_n(a_j)$ ou, ainda, que

$$\left[\binom{n}{n-1}^{-1}\sum_{i=1}^{n}a_1\ldots\widehat{a}_i\ldots a_n\right]^2\geq$$

$$\geq\left[\binom{n}{n-2}^{-1}\sum_{i<j}^{n}a_1\ldots\widehat{a}_i\ldots\widehat{a}_j\ldots a_n\right]\left[\binom{n}{n}^{-1}a_1\ldots a_n\right].$$

Sendo $P=a_1\ldots a_n$, provar a desigualdade acima equivale a provar que

$$\left(\frac{1}{n}\sum_{i=1}^{n}\frac{P}{a_i}\right)^2\geq\frac{2P}{n(n-1)}\sum_{i<j}\frac{P}{a_ia_j}$$

ou, ainda, que

$$(n-1)\left(\sum_{i=1}^{n}\frac{1}{a_i}\right)^2 \geq 2n\sum_{i<j}\frac{1}{a_ia_j}.$$

Fazendo $\alpha_i = \frac{1}{a_i}$, queremos mostrar que

$$(n-1)\left(\sum_{i=1}^{n}\alpha_i\right)^2 \geq 2n\sum_{i<j}\alpha_i\alpha_j.$$

Sendo $S = (n-1)\left(\sum_{i=1}^{n}\alpha_i\right)^2 - 2n\sum_{i<j}\alpha_i\alpha_j$, temos

$$\begin{aligned} S &= n\left(\sum_{i=1}^{n}\alpha_i\right)^2 - \left(\sum_{i=1}^{n}\alpha_i\right)^2 - 2n\sum_{i<j}\alpha_i\alpha_j \\ &= n\left[\left(\sum_{i=1}^{n}\alpha_i\right)^2 - 2\sum_{i<j}\alpha_i\alpha_j\right] - \left(\sum_{i=1}^{n}\alpha_i\right)^2 \\ &= n\sum_{i=1}^{n}\alpha_i^2 - \left(\sum_{i=1}^{n}\alpha_i\right)^2 \geq 0, \end{aligned}$$

onde a última desigualdade é simplesmente a desigualdade entre as médias quadrática e aritmética dos α_i's (veja o problema 7.3.3 de [10] ou, ainda, o teorema 6.63 de [12]).

Quanto à igualdade, se $H_{n-1}^2(a_j) = H_n(a_j)H_{n-2}(a_j)$, então, pelo que fizemos acima, temos $\alpha_1 = \cdots = \alpha_n$ e, daí, $a_1 = \cdots = a_n$. Por outro lado, se $H_i^2(a_j) = H_{i-1}(a_j)H_{i+1}(a_j)$ para algum $1 \leq i \leq n-2$, então (5.1) nos dá $H_i^2(b_j) = H_{i-1}(b_j)H_{i+1}(b_j)$. A condição de igualdade na hipótese de indução garante, agora, que $b_1 = \cdots = b_{n-1}$ e, a partir daí, é imediato que $a_1 = \cdots = a_n$. □

O corolário a seguir, usualmente imputado ao matemático escocês do século XVIII Colin McLaurin, traz o refinamento prometido da desigualdade entre as médias.

Corolário 5.11 (McLaurin). *Para $n > 1$ reais positivos $a_1, a_2, \ldots, a_n$, temos*

$$H_1(a_j) \geq \sqrt{H_2(a_j)} \geq \sqrt[3]{H_3(a_j)} \geq \cdots \geq \sqrt[n]{H_n(a_j)},$$

com igualdade em ao menos uma de tais desigualdades se, e só se, todos os a_j forem iguais.

Prova. Escreva H_j para $H_j(a_i)$. As desigualdades de Newton nos dão $H_1^2 \geq H_0H_2 = H_2$ e $H_2^2 \geq H_1H_3$. Logo, $H_1^4 \geq H_2^2 \geq H_1H_3$, de modo que $H_1^3 \geq H_3$ e, daí, $H_2^2 \geq H_1H_3 \geq H_3^{1/3}H_3 = H_3^{4/3}$. Assim, $H_1 \geq H_2^{1/2} \geq H_3^{1/3}$.

Suponha que já mostramos que

$$H_1 \geq H_2^{1/2} \geq H_3^{1/3} \geq \cdots \geq H_k^{1/k},$$

para algum $k < n$. Então,

$$H_k^2 \geq H_{k-1}H_{k+1} \geq H_k^{\frac{k-1}{k}}H_{k+1},$$

o que nos dá $H_k^{2-\left(\frac{k-1}{k}\right)} \geq H_{k+1}$ ou, ainda, $H_k^{\frac{k+1}{k}} \geq H_{k+1}$. Essa última desigualdade equivale a $H_k^{1/k} \geq H_{k+1}^{1/(k+1)}$.

Para a igualdade, suponha que $H_k^{1/k} = H_{k+1}^{1/(k+1)}$. Então, temos $H_k^2 = H_{k-1}H_{k+1}$ pois, do contrário, teríamos

$$H_k^2 > H_{k-1}H_{k+1} \geq H_k^{\frac{k-1}{k}}H_{k+1},$$

de sorte que $H_k^{2-\left(\frac{k-1}{k}\right)} > H_{k+1}$ ou, ainda, $H_k^{\frac{k+1}{k}} > H_{k+1}$, o que é uma contradição. Assim, a condição para igualdade nas desigualdades de Newton nos dá $a_1 = \cdots = a_n$. □

5.3 A regra de Descartes

O resultado principal desta seção relaciona o número de raízes positivas de um polinômio de coeficientes reais ao número de mudanças de

sinal de seus coeficientes não nulos. Dentre os resultados demonstrados anteriormente neste capítulo, sua prova utiliza somente o teorema de Bolzano e, portanto, poderia ter sido dada logo após o mesmo; contudo, adiamos sua discussão a fim de privilegiar a exposição dos resultados mais básicos, apresentados anteriormente.

Comecemos com o lema combinatório abaixo, o qual pode ser facilmente demonstrado, por indução por exemplo.

Lema 5.12. *Em relação ao alfabeto $\{+,-\}$, sejam $\mathcal{A}$ o conjunto das palavras finitas com sinais inicial e final distintos e $\mathcal{B}$ o conjunto das palavras finitas com sinais inicial e final iguais. Para cada palavra finita α, seja $\nu(\alpha)$ o número de pares de sinais consecutivos e distintos em α. Então:*

(a) $\alpha \in \mathcal{A} \Rightarrow \nu(\alpha) \equiv 1 (\text{mod } 2)$.

(b) $\alpha \in \mathcal{B} \Rightarrow \nu(\alpha) \equiv 0 (\text{mod } 2)$.

Precisamos, agora, da definição a seguir.

Definição 5.13. *Seja*

$$f(X) = a_n X^{k_n} + a_{n-1} X^{k_{n-1}} + \cdots + a_1 X^{k_1} + a_0 X^{k_0}$$

um polinômio não constante de coeficientes reais, com $k_n > k_{n-1} > \cdots > k_1 > k_0 \geq 0$ e $a_j \neq 0$ para $0 \leq j \leq n$. Defina a sequência $\nu_f = (\alpha_n, \alpha_{n-1}, \ldots, \alpha_1, \alpha_0)$ pondo, para cada inteiro $0 \leq j \leq n$,

$$\alpha_j = \begin{cases} +, & \text{se } a_j > 0 \\ -, & \text{se } a_j < 0 \end{cases}.$$

A **variação** *de f, denotada $V(f)$, é o número de pares de sinais consecutivos distintos em ν_f.*

Para nossos propósitos, o resultado a seguir é crucial.

Lema 5.14. *Seja g um polinômio não constante de coeficientes reais e $c > 0$ um real dado. Se $f(X) = (X-c)g(X)$, então $V(f) - V(g)$ é um inteiro positivo ímpar.*

Prova. Façamos indução sobre ∂g.

(a) $\partial g = 1$: é claro que podemos supor g mônico. Se $g(X) = X$, então $f(X) = X^2 - cX$, de modo que $V(f) - V(g) = 1$. Suponha, agora, $g(X) = X - \alpha$, onde $\alpha > 0$. Então, $f(X) = X^2 - (\alpha + c)X + c\alpha$, de modo que $V(f) - V(g) = 2 - 1 = 1$. O caso $g(X) = X + \alpha$, onde $\alpha > 0$, é igualmente fácil: $f(X) = X^2 + (\alpha - c)X - c\alpha$ e, como $-c\alpha < 0$, segue do lema 5.12 que $V(f)$ é ímpar. Portanto, $V(f) - V(g) = V(f)$, um inteiro positivo ímpar.

(b) Suponha o resultado válido para todo polinômio g tal que $\partial g < n$, onde $n > 1$ é inteiro, e tome um polinômio g de grau n. Dado um polinômio qualquer h, denotaremos, sempre que necessário, por α_h e β_h respectivamente o coeficiente líder de h e o coeficiente do termo de h de menor grau. Assim,

$$h(X) = \alpha_h X^r + \cdots + \beta_h X^s,$$

com $r \geq s$. Há três casos a considerar:

- Todos os coeficientes de g são positivos: supondo novamente (e sem perda de generalidade) g mônico, seja $g(X) = X^n + \cdots + \alpha X^l$, com $l < n$. Então,

$$f(X) = (X-c)g(X) = X^{n+1} + \cdots - c\alpha X^l,$$

com $c\alpha < 0$; pelo lema 5.12 concluímos que $V(f)$ é ímpar e, daí, que $V(f) - V(g) = V(f)$ é positivo e ímpar.

- Existem polinômios u e v tais que $g = u + v$, com

$$u(X) = \alpha_u X^r + \cdots + \beta_u X^s, \quad v(X) = \alpha_v X^p + \cdots + \beta_v X^q,$$

com $n = r \geq s$, $p \geq q$ e $p + 1 < s$. Então,

$$\begin{aligned}(X-c)g(X) &= (X-c)u(X) + (X-c)v(X)\\ &= (\alpha_u X^{r+1} + \cdots - c\beta_u X^s)\\ &\quad + (\alpha_v X^{p+1} + \cdots - c\beta_v X^q),\end{aligned}$$

uma vez que $p + 1 < s$. Distingamos, agora, dois subcasos: $\alpha_v\beta_u > 0$ e $\alpha_v\beta_u < 0$. No primeiro deles, temos $V(g) = V(u) + V(v)$. Porém, $(-c\beta_u)\alpha_v < 0$, de modo que, por (5.2),

$$V(f) = V((X-c)g) = V((X-c)u) + V((X-c)v) + 1.$$

Pela hipótese de indução (em princípio u tem grau $r = n$; contudo, $s > 1$ implica que podemos aplicar a hipótese de indução a $w(X) = \alpha_u X^{r-s} + \cdots + \beta_u$, uma vez $u(X) = X^s w(X)$), segue que

$$V(f) \geq (1 + V(u)) + (1 + V(v)) + 1 > V(g) + 1$$

e, módulo 2,

$$V(f) \equiv (1 + V(u)) + (1 + V(v)) + 1 \equiv V(g) + 1.$$

No segundo subcaso, $\alpha_v\beta_u < 0$, temos

$$V(g) = V(u) + V(v) + 1$$

e, por (5.2),

$$V(f) = V((X-c)g) = V((X-c)u) + V((X-c)v).$$

Usando novamente a hipótese de indução, obtemos

$$V(f) \geq (1 + V(u)) + (1 + V(v)) = V(g) + 1$$

e, módulo 2,

$$V(f) \equiv (1 + V(u)) + (1 + V(v)) \equiv V(g) + 1.$$

- $g(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_k X^k$, com $a_n, \ldots, a_k \neq 0$ e nem todos positivos: escreva

$$g = g_0 - g_1 + \cdots + (-1)^t g_t,$$

tal que cada $g_i = \alpha_i X^{k_i} + \cdots + \beta_i X^{l_i}$ $(k_i \geq l_i)$ tem todos os coeficientes positivos e, para $i < t$, $l_i = k_{i+1} + 1$. Então $V(g) = t$ e

$$\begin{aligned}(X-c)g &= (X-c)g_0 - (X-c)g_1 + \cdots + (-1)^t(X-c)g_t\\ &= (X-c)(\alpha_0 X^{k_0} + \cdots + \beta_0 X^{l_0})\\ &\quad - (X-c)(\alpha_1 X^{k_1} + \cdots + \beta_1 X^{l_1}) + \cdots\\ &\quad + (-1)^t(X-c)(\alpha_t X^{k_t} + \cdots + \beta_t X^{l_t})\\ &= \alpha_0 X^{k_0+1} + \cdots - (\alpha_1 + c\beta_0)X^{l_0} + \cdots + (\alpha_2 + c\beta_1)X^{l_1}\\ &\quad + \cdots - (\alpha_3 + c\beta_2)X^{l_2} + \cdots + (-1)^t(\alpha_t + c\beta_{t-1})X^{l_{t-1}}\\ &\quad + \cdots + (-1)^{t+1}c\beta_t X^{l_t}.\end{aligned}$$

Assim, pelo lema 5.12, há um número ímpar (e, daí, pelo menos um) de pares de coeficientes consecutivos de sinais contrários em cada um dos $t+1$ intervalos com reticências acima, de forma que

$$V(f) = V((X-c)g) \geq t + 1 = V(g) + 1;$$

segue também da observação acim que, módulo 2,

$$V(f) = V((X-c)g) \equiv t + 1 = V(g) + 1.$$

□

De posse do lema anterior, podemos enunciar e provar o resultado do teorema a seguir, o qual é conhecido como a **regra de Descartes**[4] para polinômios de coeficientes reais.

[4]Após René Descartes, matemático e filósofo francês do século XVII, conhecido como o pai da Geometria Analítica.

Teorema 5.15. *Seja f um polinômio não constante de coeficientes reais. Se $\mathcal{R}_+(f)$ denota o número de raízes positivas de f, então $V(f) - \mathcal{R}_+(f)$ é um inteiro par e não negativo.*

Prova. Façamos indução sobre o grau de f.

Se $\partial f = 1$ suponhamos, sem perda de generalidade, que f é mônico. Se $f(X) = X$ ou $f(X) = X + \alpha$, com $\alpha > 0$, então $V(f) - \mathcal{R}_+(f) = 0 - 0 = 0$. Se $f(X) = X - \alpha$, com $\alpha > 0$, então $V(f) - \mathcal{R}_+(f) = 1 - 1 = 0$.

Suponha, agora, o teorema válido para todo polinômio de grau menor que n, onde $n > 1$ é inteiro, e seja

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

um polinômio de grau n. Há dois casos a considerar:

- $\mathcal{R}_+(f) = 0$: nesse caso, basta mostrar que $V(f)$ é par. Como $f(0) = a_0$ e $f(x)$ tem o sinal de a_n para todo real x suficientemente grande (por uma estimativa análoga àquela que precede 3.7)), o fato de que $\mathcal{R}_+(f) = 0$ garante, via teorema de Bolzano, que $a_na_0 > 0$; daí, o lema 5.12 garante que $V(f)$ é par.

- $\mathcal{R}_+(f) > 0$: tomando uma raiz positiva c de f, existe um polinômio não constante g tal que $f(X) = (X - c)g(X)$. O lema 5.14 garante a existência de um inteiro ímpar e positivo I, tal que

$$\begin{aligned} V(f) - \mathcal{R}_+(f) &= (V(g) + I) - (\mathcal{R}_+(g) + 1) \\ &= (V(g) - \mathcal{R}_+(g)) + (I - 1). \end{aligned}$$

Como, pela hipótese de indução, $V(g) - \mathcal{R}_+(g)$ é par e não negativo, segue que $V(f) - \mathcal{R}_+(f)$ é também par e não negativo.

□

Corolário 5.16. *Se f é um polinômio não constante de coeficientes reais e $\mathcal{R}_-(f)$ é o número de raízes negativas de f, então $V(f(-X)) - \mathcal{R}_-(f)$ é par e não negativo.*

Prova. Imediata, a partir do teorema 5.15, juntamente com o fato de que $\alpha \in \mathcal{R}_-(f)$ se, e só se, $-\alpha \in \mathcal{R}_+(f)$. □

Exemplo 5.17. *Sejam $a_0, a_1, \ldots, a_{n-1}$ reais não negativos e não todos nulos. Calcule o número de raízes positivas do polinômio*

$$X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0.$$

Solução. Se f denota o polinômio do enunciado, a regra de Descartes garante que $V(f) - \mathcal{R}_+(f)$ é não negativo e par. Mas, como $V(f) = 1$, é imediato que $\mathcal{R}_+(f) = 1$. □

Problemas – Seção 5.3

1. Para cada $n \in \mathbb{N}$, seja a_n uma raiz real positiva do polinômio $X^n - X^{n-1} - X^{n-2} - \cdots - X - 1$. Mostre que, para todo tal n, temos
$$2 - \frac{1}{2^{n-1}} \leq a_n \leq 2 - \frac{1}{2^n}.$$

2. (Leningrado.) O polinômio de terceiro grau e coeficientes reais $aX^3 + bX^2 + cX + d$ tem três raízes reais distintas. Calcule o número de raízes reais do polinômio
$$4(aX^3 + bX^2 + cX + d)(3aX + b) - (3aX^2 + 2bX + c)^2.$$

CAPÍTULO 6

Interpolação de Polinômios

O corolário 3.10 garante que há, no máximo, um polinômio de grau n que assume valores predeterminados em $n + 1$ valores complexos distintos da variável. O que não sabemos ainda é se um tal polinômio realmente existe. Por exemplo, há um polinômio f de coeficientes racionais, grau 3 e satisfazendo as condições $f(0) = 1$, $f(1) = 2$, $f(2) = 3$ e $f(3) = 0$? Estudaremos, aqui, técnicas que possibilitam responder essa pergunta, técnicas essas denominadas genericamente de **interpolação de polinômios**. Em especial, discutiremos a classe dos polinômios interpoladores de Lagrange, os quais serão, por sua vez, utilizados para resolver sistemas lineares de Vandermonde sem o recurso aos métodos da Álgebra Linear. A seu turno, o conhecimento das soluções de um tal sistema nos possibilitará estudar, na seção 9.1, uma classe particular importante de sequências recorrentes lineares, estendendo parcialmente o material da seção 4.3 de [10].

6.1 Bases para polinômios

Para o que segue, lembre-se de que $\mathbb{K}$ representa um qualquer dos conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Precisamos, inicialmente, estabelecer uma convenção útil.

Notação 6.1. *Para $n \in \mathbb{N}$ e $1 \leq i, j \leq n$, definimos o* **delta de Kronecker**[1] *por*

$$\delta_{ij} = \begin{cases} 1, & se\ i = j \\ 0, & se\ i \neq j \end{cases}.$$

A vantagem da notação acima vem do fato de podermos usá-la como um **marcador de posições**, no seguinte sentido: dados $n \in \mathbb{N}$ e uma sequência $(b_1, \ldots, b_n)$ em $\mathbb{K}$, temos

$$\sum_{j=1}^{n} \delta_{ij} b_j = b_i,$$

para $1 \leq i \leq n$.

Agora, sejam dados $n \in \mathbb{N}$ e elementos dois a dois distintos a_1, a_2, $\ldots$, a_n de $\mathbb{K}$. Para $1 \leq i \leq n$, definimos o polinômio $L_i \in \mathbb{K}[X]$ por

$$L_i(X) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j} = \left(\frac{X - a_1}{a_i - a_1}\right) \cdots \widehat{\left(\frac{X - a_i}{a_i - a_i}\right)} \cdots \left(\frac{X - a_n}{a_i - a_n}\right),$$

onde o sinal $\widehat{\ }$ sobre um fator indica que o mesmo está ausente do produto considerado. Tais polinômios L_i são os **polinômios interpoladores de Lagrange** para o conjunto $\{a_1, \ldots, a_n\}$.

É imediato verificar que, para todos $1 \leq i, j \leq n$, tem-se

$$L_i(a_j) = \delta_{ij}.$$

[1] Após o matemático alemão do século XIX Leopold Kronecker.

Essa propriedade permite, como veremos no teorema a seguir, construir polinômios que assumam valores pré-fixados em elementos distintos de $\mathbb{K}$ também pré-fixados; tal resultado é conhecido como o **teorema de interpolação de Lagrange**.

Teorema 6.2 (Lagrange). *Dados $n \in \mathbb{N}$ e $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{K}$, com $a_1, \ldots, a_n$ dois a dois distintos, existe exatamente um polinômio $f \in \mathbb{K}[X]$, de grau menor que n e tal que $f(a_i) = b_i$, para $1 \leq i \leq n$. Mais precisamente, tal polinômio é*

$$f(X) = \sum_{j=1}^{n} b_j L_j(X), \tag{6.1}$$

onde os L_j são os polinômios interpoladores de Lagrange para o subconjunto $\{a_1, \ldots, a_n\}$ de $\mathbb{K}$.

Prova. A unicidade segue do corolário 3.10. Por outro lado, tomando f como em (6.1), basta mostrarmos que $\partial f < n$ e $f(a_i) = b_i$, para $1 \leq i \leq n$.

Como $\partial L_j = n - 1$ para $1 \leq j \leq n$ e o grau de uma soma de polinômios (sempre que tal soma for não nula) não ultrapassa o maior dentre os graus das parcelas, é imediato que $\partial f < n$. Para o que falta, basta ver que

$$f(a_i) = \sum_{j=1}^{n} b_j L_j(a_i) = \sum_{j=1}^{n} b_j \delta_{ji} = b_i.$$

□

Uma maneira equivalente de formular o resultado acima é dada pelo corolário a seguir.

Corolário 6.3. *Sejam $n \in \mathbb{N}$ e $a_1, \ldots, a_n$ elementos dois a dois distintos de $\mathbb{K}$. Se $f \in \mathbb{K}[X] \setminus \{0\}$ satisfaz $\partial f < n$, então*

$$f(X) = \sum_{i=1}^{n} f(a_i) L_i(X).$$

Prova. De fato, definindo

$$g(X) = \sum_{i=1}^{n} f(a_i)L_i(X),$$

temos $\partial f, \partial g < n$ e, pela demonstração do teorema anterior, $g(a_i) = f(a_i)$, para $1 \leq i \leq n$. Segue novamente do corolário 3.10 que $g = f$. □

Colecionamos, a seguir, dois exemplos de aplicação dos polinômios interpoladores de Lagrange.

Exemplo 6.4. *Encontre um polinômio* $f \in \mathbb{Q}[X]$ *tal que* $f(1) = 12$, $f(2) = 2$, $f(3) = 1$, $f(4) = -6$ *e* $f(5) = 4$.

Solução. Explicitemos, primeiramente, os polinômios interpoladores de Lagrange para o conjunto $\{1, 2, 3, 4, 5\}$:

$$\begin{aligned} L_1(X) &= \prod_{\substack{1\leq j\leq 5\\ j\neq 1}} \frac{X-j}{1-j} = \left(\frac{X-2}{1-2}\right)\left(\frac{X-3}{1-3}\right)\left(\frac{X-4}{1-4}\right)\left(\frac{X-5}{1-5}\right) \\ &= \frac{1}{24}(X^4 - 14X^3 + 71X^2 - 154X + 120), \end{aligned}$$

$$\begin{aligned} L_2(X) &= \prod_{\substack{1\leq j\leq 5\\ j\neq 2}} \frac{X-j}{2-j} = \left(\frac{X-1}{2-1}\right)\left(\frac{X-3}{2-3}\right)\left(\frac{X-4}{2-4}\right)\left(\frac{X-5}{2-5}\right) \\ &= -\frac{1}{6}(X^4 - 13X^3 + 59X^2 - 107X + 60), \end{aligned}$$

$$\begin{aligned} L_3(X) &= \prod_{\substack{1\leq j\leq 5\\ j\neq 3}} \frac{X-j}{3-j} = \left(\frac{X-1}{3-1}\right)\left(\frac{X-2}{3-2}\right)\left(\frac{X-4}{3-4}\right)\left(\frac{X-5}{3-5}\right) \\ &= \frac{1}{4}(X^4 - 12X^3 + 49X^2 - 78X + 40), \end{aligned}$$

$$\begin{aligned} L_4(X) &= \prod_{\substack{1\leq j\leq 5\\ j\neq 4}} \frac{X-j}{4-j} = \left(\frac{X-1}{4-1}\right)\left(\frac{X-2}{4-2}\right)\left(\frac{X-3}{4-3}\right)\left(\frac{X-5}{4-5}\right) \\ &= -\frac{1}{6}(X^4 - 11X^3 + 41X^2 - 61X + 30) \end{aligned}$$

e

$$\begin{aligned} L_5(X) &= \prod_{\substack{1\leq j\leq 5\\ j\neq 5}} \frac{X-j}{5-j} = \left(\frac{X-1}{5-1}\right)\left(\frac{X-2}{5-2}\right)\left(\frac{X-3}{5-3}\right)\left(\frac{X-4}{5-4}\right) \\ &= \frac{1}{24}(X^4 - 10X^3 + 35X^2 - 50X + 24). \end{aligned}$$

Portanto, de acordo com o corolário anterior podemos tomar

$$\begin{aligned} f(X) &= 12L_1(X) + 2L_2(X) + L_3(X) - 6L_4(X) + 4L_5(X) \\ &= \frac{19}{12}X^4 - \frac{55}{3}X^3 + \frac{233}{4}X^2 - \frac{775}{6}X + 86. \end{aligned}$$

□

Exemplo 6.5. *Seja* f *um polinômio mônico, de coeficientes reais e grau* n, *e sejam* $x_1, x_2, \ldots, x_{n+1}$ *inteiros dois a dois distintos. Prove que existe* $1 \leq k \leq n+1$ *tal que* $|f(x_k)| \geq \frac{n!}{2^n}$.

Prova. Pela fórmula de interpolação de Lagrange, temos

$$f(x) = \sum_{j=1}^{n+1} f(x_j) \prod_{i\neq j} \frac{x - x_i}{x_j - x_i}.$$

Comparando os coeficientes líderes nos dois membros da igualdade acima, obtemos

$$1 = \sum_{j=1}^{n+1} \frac{f(x_j)}{\prod_{i\neq j}(x_j - x_i)}.$$

Agora, se $M = \max\{|f(x_k)|;\, 1 \leq k \leq n+1\}$ e $p_j = \prod_{i \neq j}(x_j - x_i)$, temos

$$1 = \left|\sum_{j=1}^{n+1} \frac{f(x_j)}{p_j}\right| \leq \sum_{j=1}^{n+1} \frac{|f(x_j)|}{|p_j|} \leq M \sum_{j=1}^{n+1} \frac{1}{|p_j|}.$$

Mas, como $\sum_{j=1}^{n+1} \frac{1}{|p_j|}$ é simétrico em relação a $x_1, x_2, \ldots, x_{n+1}$, podemos supor (após reenumerar os x_i's, se necessário) que $x_1 < x_2 < \cdots < x_{n+1}$. Assim,

$$\begin{aligned} |p_j| &= (x_j - x_1)\ldots(x_j - x_{j-1})(x_{j+1} - x_j)\ldots(x_{n+1} - x_j) \\ &\geq [(j-1)\ldots 2 \cdot 1][1 \cdot 2 \ldots (n+1-j)] \\ &= (j-1)!(n+1-j)! = \frac{n!}{\binom{n}{j-1}}. \end{aligned}$$

De posse das estimativas acima, obtemos finalmente

$$1 \leq M \sum_{j=1}^{n+1} \frac{1}{|p_j|} \leq M \sum_{j=1}^{n+1} \frac{1}{n!}\binom{n}{j-1} = \frac{2^n M}{n!}$$

ou, o que é o mesmo, $M \geq \frac{n!}{2^n}$. □

A seguir, mostramos como utilizar polinômios interpoladores de Lagrange para resolver certos tipos de sistemas lineares de equações, ditos **sistemas de Vandermonde**[2], os quais encontrarão utilidade na seção 9.1.

Proposição 6.6 (Vandermonde). *Dados elementos $a_1, a_2, \ldots, a_n$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ de $\mathbb{K}$, sendo $a_1, a_2, \ldots, a_n$ dois a dois distintos, o sistema linear de equações*

$$\left\{\begin{array}{lcl} x_1 + x_2 + \cdots + x_n & = & \alpha_1 \\ a_1x_1 + a_2x_2 + \cdots + a_nx_n & = & \alpha_2 \\ a_1^2x_1 + a_2^2x_2 + \cdots + a_n^2x_n & = & \alpha_3 \\ \cdots & & \\ a_1^{n-1}x_1 + a_2^{n-1}x_2 + \cdots + a_n^{n-1}x_n & = & \alpha_n \end{array}\right. \tag{6.2}$$

[2]Alexandre-Théophile Vandermonde, matemático francês do século XVIII.

admite uma única solução em $\mathbb{K}$. Em particular, se $\alpha_1 = \cdots = \alpha_n = 0$, então $x_1 = \cdots = x_n = 0$.

Prova. Se $f(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in \mathbb{K}[X]$, então, multiplicando as equações do sistema respectivamente por $c_0, c_1, \ldots, c_{n-1}$ e somando os resultados, obtemos

$$f(a_1)x_1 + \cdots + f(a_n)x_n = c_0\alpha_1 + c_1\alpha_2 + \cdots + c_{n-1}\alpha_n.$$

Agora, fixado $1 \leq i \leq n$, o teorema 6.2 nos permite escolher unicamente $c_0, c_1, \ldots, c_{n-1}$ em $\mathbb{K}$ (i.e., escolher f) de modo que $f(a_1) = \cdots = \widehat{f(a_i)} = \cdots = f(a_n) = 0$ e $f(a_i) = 1$. Portanto, a igualdade acima garante que deve ser

$$x_i = c_0\alpha_1 + c_1\alpha_2 + \cdots + c_{n-1}\alpha_n \in \mathbb{K},$$

e a arbitrariedade do $1 \leq i \leq n$ escolhido termina a demonstração. □

Uma limitação dos polinômios interpoladores de Lagrange para um subconjunto finito de $\mathbb{K}$ vem do fato de que, com eles, só geramos o conjuto dos polinômios de graus menores que o número de elementos do conjunto em questão. Remediamos essa situação com a seguinte definição mais geral.

Definição 6.7. *Uma* **base** *para $\mathbb{K}[X]$ é uma sequência*[3] *$(f_0, f_1, f_2, \ldots)$ de elementos de $\mathbb{K}[X]$ satisfazendo a seguinte condição: para todo $f \in \mathbb{K}[X]$, existem únicos $n \in \mathbb{Z}_+$ e $a_0, \ldots, a_n \in \mathbb{K}$ tais que*

$$f(X) = a_0f_0(X) + \cdots + a_nf_n(X).$$

Exemplo 6.8. *Uma maneira simples de construir uma base para $\mathbb{K}[X]$ é tomar uma sequência $(f_0, f_1, f_2, \ldots)$ de $\mathbb{K}[X]$ tal que $\partial f_j = j$, para*

[3]Formalmente, uma sequência $(f_j)_{j \geq 0}$ em $\mathbb{K}[X]$ é uma função $\Phi : \mathbb{Z}_+ \to \mathbb{K}[X]$, tal que $f_j = \Phi(j)$, para $j \geq 0$.

$j \geq 0$. *Para mostrar que um tal sequência é realmente uma base para* $\mathbb{K}[X]$, *temos de provar as duas afirmações a seguir:*

(i) Se $a_0, a_1, \ldots, a_n$ *e* $b_0, b_1, \ldots, b_n$ *são elementos de* $\mathbb{K}$ *tais que*

$$a_0 f_0(X) + a_1 f_1(X) + \cdots + a_n f_n(X) = b_0 f_0(X) + b_1 f_1(X) + \cdots + b_n f_n(X),$$

então $a_i = b_i$, *para* $0 \leq i \leq n$.

(ii) Para todo $f \in \mathbb{K}[X]$, *existem* $n \in \mathbb{N}$ *e* $a_0, a_1, \ldots, a_n \in \mathbb{K}$, *tais que*

$$f(X) = a_0 f_0(X) + a_1 f_1(X) + \cdots + a_n f_n(X).$$

Deixamos ao leitor a verificação de que a validade das afirmações dos itens (i) e (ii) acima é realmente equivalente ao fato de que tal sequência de polinômios é uma base (veja o problema 1).

Como caso particular do exemplo acima, note que a sequência

$$(1, X, X^2, X^3, \ldots)$$

é uma base para $\mathbb{K}[X]$ (como, aliás, já sabíamos).

No que segue, construímos, a partir dos números binomiais, uma base bastante útil para $\mathbb{K}[X]$. Para tanto, precisamos da definição a seguir.

Definição 6.9. *Para* $k \in \mathbb{Z}_+$, *definimos o* k*-ésimo* **polinômio binomial** $\binom{X}{k}$ *por* $\binom{X}{0} = 1$, $\binom{X}{1} = X$ *e, para* $k > 1$,

$$\binom{X}{k} = \frac{1}{k!} X(X-1)\ldots(X-k+1).$$

Como aplicação do exemplo 6.8, afirmamos que a sequência dos polinômios binomiais é uma base para $\mathbb{K}[X]$. Para tanto, basta mostrarmos que as condições dos itens (i) e (ii) são satisfeitas. A verificação da validade da condição (i) segue, como no exemplo 6.8, do fato

de que $\partial\binom{X}{k} = k$, para todo $k \in \mathbb{Z}_+$. Quanto a (ii), basta mostrarmos que, para todo $n \in \mathbb{Z}_+$, existem $a_0, a_1, \ldots, a_n \in \mathbb{K}$ tais que

$$X^n = a_0\binom{X}{0} + a_1\binom{X}{1} + \cdots + a_n\binom{X}{n}. \tag{6.3}$$

Sem apelar diretamente para o resultado do exemplo supracitado, façamos indução sobre $n \geq 0$. Para $n = 0$ e $n = 1$, a validez de (6.3) segue da definição de polinômio binomial. Suponha agora que, para um certo $k \in \mathbb{N}$, existam $a_0, a_1, \ldots, a_k \in \mathbb{K}$ satisfazendo (6.3) quando $n = k$. Então,

$$a_0\binom{X}{0}X + a_1\binom{X}{1}X + \cdots + a_k\binom{X}{k}X = X^{k+1} \tag{6.4}$$

e, para terminar, basta ver que

$$\begin{aligned}\binom{X}{j}X &= \frac{1}{j!}X(X-1)\ldots(X-j+1)(X-j+j)\\ &= \frac{1}{j!}X(X-1)\ldots(X-j+1)(X-j)\\ &\quad+\frac{j}{j!}X(X-1)\ldots(X-j+1)\\ &= (j+1)\binom{X}{j+1} + j\binom{X}{j}.\end{aligned}$$

Ainda que o conceito de base de polinômios, conforme formulado nesta seção, não se aplique ao conjunto dos polinômios de coeficientes inteiros, uma rápida revisão da discussão acima estabelece o seguinte resultado mais geral.

Proposição 6.10. *Se* $f \in \mathbb{K}[X]\setminus\{0\}$ *é um polinômio de grau* n, *então existem únicos* $a_0, a_1, \ldots, a_n \in \mathbb{K}$ *tais que*

$$f(X) = a_0\binom{X}{0} + a_1\binom{X}{1} + \cdots + a_n\binom{X}{n}.$$

Ademais, se $f \in \mathbb{Z}[X]$, *então podemos tomar* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$.

Prova. É suficiente provar que os coeficientes $a_0, a_1, \ldots, a_n$ em (6.3) são inteiros. Argumentando novamente por indução, suponha que tal afirmação é verdadeira quando $n = k$. Então, os cálculos subsequentes a (6.4) fornecem

$$\begin{aligned} X^{k+1} &= \sum_{j=0}^{k} a_j \binom{X}{j} X \\ &= \sum_{j=0}^{k} a_j \left((j+1)\binom{X}{j+1} + j\binom{X}{j}\right) \\ &= \sum_{j=0}^{k+1} j(a_{j-1} + a_j)\binom{X}{j}, \end{aligned}$$

com $a_{-1} = a_{k+1} = 0$. Portanto, $a_j \in \mathbb{Z}$, para $0 \leq j \leq k+1$, de forma que $j(a_{j-1} + a_j) \in \mathbb{Z}$, para $0 \leq j \leq k+1$, completando o passo de indução. □

Vejamos um exemplo interessante de aplicação das ideias discutidas acima.

Exemplo 6.11. *Seja $f \in \mathbb{R}[X]$ um polinômio de grau n e suponha que $f(0), f(1), \ldots, f(n)$ sejam inteiros. Prove que $f(x)$ é inteiro para todo inteiro x.*

Prova. Pela proposição acima, existem $a_0, a_1, \ldots, a_n \in \mathbb{R}$ tais que

$$f(X) = a_0\binom{X}{0} + a_1\binom{X}{1} + \cdots + a_n\binom{X}{n}. \tag{6.5}$$

Portanto, para $0 \leq k \leq n$ fixado, temos

$$f(k) = \sum_{j=0}^{n} a_j \binom{X}{j}(k) = \sum_{j=0}^{k} \binom{k}{j} a_j$$

(uma vez que $\binom{X}{j}(k) = 0$ se $j > k$). Agora, aplicando o lema 2.12 de [13], concluímos que

$$a_k = \sum_{j=0}^{k} (-1)^{k+j} \binom{k}{j} f(j) \in \mathbb{Z},$$

para $0 \leq k \leq n$. Mas, uma vez que $\binom{X}{k}(x) \in \mathbb{Z}$ para todo $x \in \mathbb{Z}$ (veja o problema 2), segue de (6.5) que $f(x) \in \mathbb{Z}$, para todo $x \in \mathbb{Z}$. □

Problemas – Seção 6.1

1. * Termine a discussão do exemplo 6.8.
2. * Para $k \in \mathbb{Z}_+$, prove que $\binom{X}{k}(x) \in \mathbb{Z}$, para todo $x \in \mathbb{Z}$.
3. (Estados Unidos.) Seja f um polinômio de grau n, tal que $f(k) = \binom{n+1}{k}^{-1}$ para $0 \leq k \leq n$. Calcule $f(n+1)$.
4. (Canadá.) Seja f um polinômio de grau n, tal que $f(k) = \frac{k}{k+1}$ para todo inteiro $0 \leq k \leq n$. Calcule $f(n+1)$.
5. Seja n um natural dado.

   (a) Mostre que $0, -1, -2, \ldots, -n$ são raízes do polinômio

   $$f(X) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} X(X+1)\ldots\widehat{(X+j)}\ldots(X+n) - n!.$$

   (b) Conclua, a partir de (a), que, para todo $k \in \mathbb{N}$, tem-se

   $$\sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{1}{k+j} = \frac{n!}{k(k+1)\ldots(k+n)}.$$

(c) Use o item (b) para calcular, em função de n, o valor da soma

$$\sum_{k\geq 1}\frac{1}{k(k+1)\dots(k+n)}.$$

6. Dados números reais dois a dois distintos a, b, c e d, resolva o sistema de equações

$$\begin{cases} ax_1+a^2x_2+a^3x_3+a^4x_4 &= 1\\ bx_1+b^2x_2+b^3x_3+b^4x_4 &= 1\\ cx_1+c^2x_2+c^3x_3+c^4x_4 &= 1\\ dx_1+d^2x_2+d^3x_3+d^4x_4 &= 1\end{cases}.$$

7. (Estados Unidos.) Sejam $n>3$ inteiro e p, p_0, p_1, $\dots$, p_{n-2} polinômios tais que

$$\sum_{j=0}^{n-2}X^jp_j(X^n)=(X^{n-1}+X^{n-2}+\cdots+X+1)p(X).$$

Prove que $X-1$ divide $p_j(X)$, para $0\leq i\leq n-2$.

8. (Leningrado.) Uma sequência finita $a_1,a_2,\dots,a_n$ é $p-$*balanceada* se todas as somas da forma

$$a_k+a_{k+p}+a_{k+2p}+\cdots$$

forem, para $k=1,2,\dots,p$, iguais entre si. Prove que, se $n=50$ e a sequência $(a_j)_{1\leq j\leq 50}$ for $p-$balanceada para $p=3$, 5, 7, 11, 13 e 17, então todos os seus termos são iguais a zero.

6.2 Diferenças finitas

Outra técnica de interpolação útil, mas um tanto mais elaborada, é a das *diferenças finitas*. Esboçamos os rudimentos da mesma nesta seção.

Definição 6.12. *Sejam h um número real e $f:\mathbb{R}\to\mathbb{R}$ uma função dada. Para $k\geq 0$ inteiro, definimos a $k-$ésima* **diferença finita** *de f com incremento h como a função $\Delta_h^kf:\mathbb{R}\to\mathbb{R}$, dada por:*

(a) $\Delta_h^0f=f$.

(b) $(\Delta_h^1f)(x)=(\Delta_hf)(x)=f(x+h)-f(x)$, para todo $x\in\mathbb{R}$.

(c) $\Delta_h^kf=\Delta_h(\Delta_h^{k-1}f)$, se $k\geq 2$.

A fim de que tal definição tenha utilidade, precisamos das propriedades de Δ_h^kf contidas na proposição a seguir.

Proposição 6.13. *Nas notações da definição anterior, dados $h\in\mathbb{R}$ e $f,g:\mathbb{R}\to\mathbb{R}$, temos que:*

(a) Se f é constante, então $\Delta_hf=0$.

(b) Se a e b são constantes reais, então $\Delta_h(af+bg)=a\Delta_hf+b\Delta_hg$.

(c) $\Delta_h(fg)=(\Delta_hf)(g+\Delta_hg)+f\Delta_hg$.

(d) $\Delta_h^kf=\Delta_h^{k-1}(\Delta_hf)$, para todo $k\in\mathbb{N}$.

(e) Se $k\geq 0$ e $x\in\mathbb{R}$, então

$$(\Delta_h^kf)(x)=\sum_{j=0}^{k}(-1)^j\binom{k}{j}f(x+(k-j)h).$$

Prova.
(a) Para $x\in\mathbb{R}$, temos $\Delta_hf(x)=f(x+h)-f(x)=0$, uma vez que f é constante.

(b) Para $x\in\mathbb{R}$, temos

$$\begin{aligned}(\Delta_h(af+bg))(x) &= (af+bg)(x+h)-(af+bg)(x)\\ &= a(f(x+h)-f(x))+b(g(x+h)-g(x))\\ &= a(\Delta_hf)(x)+b(\Delta_hg)(x).\end{aligned}$$

(c) Façamos indução sobre $k \geq 1$, sendo o caso $k = 1$ imediato. Suponha, por hipótese de indução, que a fórmula valha para um certo $k \in \mathbb{N}$. Para $k+1$, temos:

$$\begin{aligned} f(x+(k+1)h) &= f(x+kh) + (\Delta_h^1 f)(x+kh) \\ &= f(x+kh) + \sum_{j=0}^{k} \binom{k}{j} (\Delta_h^{k-j}(\Delta_h^1 f))(x) \\ &= \sum_{j=0}^{k} \binom{k}{j} (\Delta_h^{k-j} f)(x) + \sum_{j=0}^{k} \binom{k}{j} (\Delta_h^{k+1-j} f)(x) \\ &= \sum_{j=0}^{k} \binom{k}{j} (\Delta_h^{k-j} f)(x) + (\Delta_h^{k+1} f)(x) \\ &\quad + \sum_{j=1}^{k} \binom{k}{j} (\Delta_h^{k-(j-1)} f)(x). \end{aligned}$$

Agora, executando uma troca de índices na última soma acima e utilizando a relação de Stifel, obtemos $f(x+(k+1)h)$ sucessivamente igual a

$$\begin{aligned} &\sum_{j=0}^{k} \binom{k}{j} (\Delta_h^{k-j} f)(x) + (\Delta_h^{k+1} f)(x) + \sum_{j=0}^{k-1} \binom{k}{j+1} (\Delta^{k-j} f)(x) \\ &= (\Delta_h^{k+1} f)(x) + \sum_{j=0}^{k-1} \left(\binom{k}{j} + \binom{k}{j+1} \right) (\Delta_h^{(k+1)-(j+1)} f)(x) + (\Delta_h^0 f)(x) \\ &= \sum_{j=0}^{k+1} \binom{k+1}{j} (\Delta_h^{k+1-j} f)(x). \end{aligned}$$

(d) Façamos indução sobre $k \geq 1$, sendo o caso $k = 1$ imediato a partir da definição 6.12. Suponha, por hipótese de indução, o resultado verdadeiro quando $k = l \geq 1$. Para $k = l+1$, aplicando sucessivamente a o item (c) da definição 6.12, a hipótese de indução e novamente o item (c) da definição 6.12 (desta feita à função $\Delta_h f$, no lugar de f), obtemos

$$\Delta_h^{l+1} f = \Delta_h(\Delta_h^l f) = \Delta_h(\Delta_h^{l-1}(\Delta_h f)) = \Delta_h^l(\Delta_h f).$$

(e) Façamos indução sobre $k \geq 0$. Se $k = 0$ e $x \in \mathbb{R}$, então

$$\sum_{j=0}^{0} (-1)^j \binom{0}{j} f(x) = (-1)^0 \binom{0}{0} f(x) = f(x) = (\Delta_h^0 f)(x).$$

Suponhamos, agora, que a fórmula valha quando $k = l \geq 0$, e provemos sua validade para $k = l+1$. Para $x \in \mathbb{R}$, aplicando sucessivamente o item (c) da definição 6.12 e a hipótese de indução, obtemos

$$\begin{aligned} (\Delta^{l+1} f)(x) &= \Delta_h(\Delta_h^l f)(x) = (\Delta_h^l f)(x+h) - (\Delta_h^l f)(x) \\ &= \sum_{j=0}^{l} (-1)^j \binom{l}{j} f(x+h+(l-j)h) \\ &\quad - \sum_{j=0}^{l} (-1)^j \binom{l}{j} f(x+(l-j)h) \\ &= f(x+(l+1)h) \\ &\quad + \sum_{j=1}^{l} (-1)^j \left(\binom{l+1}{j} - \binom{l}{j-1} \right) f(x+(l+1-j)h) \\ &\quad - \sum_{j=0}^{l} (-1)^j \binom{l}{j} f(x+(l-j)h) \\ &= \sum_{j=0}^{l} (-1)^j \binom{l+1}{j} f(x+(l+1-j)h) \\ &\quad - \sum_{j=1}^{l} (-1)^j \binom{l}{j-1} f(x+(l+1-j)h) \\ &\quad - \sum_{j=0}^{l} (-1)^j \binom{l}{j} f(x+(l-j)h), \end{aligned}$$

onde utilizamos a relação de Stifel (6.2) de [10] na penúltima igualdade acima. Portanto,

$$\begin{aligned}
\Delta^{l+1} f(x) &= \sum_{j=0}^{l+1}(-1)^j \binom{l+1}{j} f(x+(l+1-j)h) - (-1)^{l+1} f(x) \\
&\quad + \sum_{j=0}^{l-1}(-1)^j \binom{l}{j} f(x+(l-j)h) \\
&\quad , \sum_{j=0}^{l}(-1)^j \binom{l}{j} f(x+(l-j)h) \\
&= \sum_{j=0}^{l+1}(-1)^j \binom{l+1}{j} f(x+(l+1-j)h) \\
&\quad + \sum_{j=0}^{l}(-1)^j \binom{l}{j} f(x+(l-j)h) \\
&\quad - \sum_{j=0}^{l}(-1)^j \binom{l}{j} f(x+(l-j)h) \\
&= \sum_{j=0}^{l+1}(-1)^j \binom{l+1}{j} f(x+(l+1-j)h).
\end{aligned}$$

□

Dentre as propriedades de diferenças finitas elencadas na proposição acima, a que encontra uso mais frequente em problemas de interpolação é a do item (e), principalmente quando combinada com o próximo resultado. Note que a proposição anterior se refere a diferenças finitas de funções em geral, ao passo que o que segue é especificamente relacionado a diferenças finitas de polinômios.

Proposição 6.14. *As $k-$ésimas diferenças finitas, com incremento h, de um polinômio de coeficientes reais e grau k são todas iguais entre*

si, ao passo que as $l-$ésimas diferenças, com $l > k$, são todas iguais a zero.

Prova. Para $x \in \mathbb{R}$, temos

$$(\Delta_h f)(x) = f(x+h) - f(x),$$

e este é o valor do polinômio $\Delta_h f(X) := f(X+h) - f(X)$ para $X = x$. Agora, observe que $\Delta_h f(X)$ tem grau $k-1$. Portanto, argumentando por indução sobre o grau de um polinômio, segue do item (d) da proposição anterior que $\Delta_h^k f = \Delta_h^{k-1}(\Delta_h f)$ tem grau 0, de sorte que é constante. Logo, $\Delta_h^l f(X) = 0$ para $l > k$. □

Conforme ficará patente nos dois exemplos a seguir, a principal utilidade das fórmulas para diferenças finitas discutidas acima é o fato de as mesmas nos permitirem calcular diretamente o valor que um polinômio assume em um ponto que não os de interpolação, caso tais pontos de interpolação sejam os termos de uma progressão aritmética.

Exemplo 6.15. *Seja $f \in \mathbb{R}[X]$ um polinômio de grau $m \geq 1$, tal que $f(j) = r^j$ para $0 \leq j \leq m$, onde r é um real positivo dado. Calcule os possíveis valores de $f(m+1)$.*

Solução. Ponha $h = 1$ e escreva $\Delta^k f$ para denotar $\Delta_1^k f$. O item (e) da proposição 6.13 garante que

$$\Delta^k f(x) = \sum_{j=0}^{k}(-1)^j \binom{k}{j} f(x+k-j)$$

para todo $x \in \mathbb{R}$. Mas, uma vez que $\partial f = m$, a proposição anterior nos dá, então,

$$0 = \Delta^{m+1} f(0) = \sum_{j=0}^{m+1}(-1)^j \binom{m+1}{j} f(m+1-j).$$

Portanto,

$$\begin{aligned} f(m+1) &= \sum_{j=1}^{m+1}(-1)^{j+1}\binom{m+1}{j}f(m+1-j) \\ &= \sum_{j=1}^{m+1}(-1)^{j+1}\binom{m+1}{j}r^{m+1-j} \\ &= r^{m+1} - \sum_{j=0}^{m+1}(-1)^{j}\binom{m+1}{j}r^{m+1-j} \\ &= r^{m+1} - (r-1)^{m+1}, \end{aligned}$$

onde utilizamos a fórmula de expansão binomial de $(r-1)^{m+1}$ na última igualdade acima. □

A solução do próximo exemplo utiliza livremente alguns conceitos e resultados básicos de Teoria dos Números, os quais podem ser encontrados em [14].

Exemplo 6.16. *Seja f um polinômio de grau 1992, tal que $f(j) = 2^j$ para $1 \leq i \leq 1993$. Calcule o resto da divisão de $f(1994)$ por 1994.*

Solução. Combinando o item (e) da proposição 6.13 com a proposição 6.14, e escrevendo novamente $\Delta^k f$ para denotar $\Delta_1^k f$, temos

$$0 = \Delta^{1993}f(1) = \sum_{j=0}^{1993}(-1)^j\binom{1993}{j}f(1994-j).$$

Portanto,

$$\begin{aligned} f(1994) &= \sum_{j=1}^{1993}(-1)^{j+1}\binom{1993}{j}2^{1994-j} \\ &= \binom{1993}{0}2^{1994} - 2\sum_{j=0}^{1993}(-1)^j\binom{1993}{j}2^{1993-j} \\ &= 2^{1994} - 2(2-1)^{1993} = 2^{1994} - 2. \end{aligned}$$

Para o que falta, note inicialmente que 997 é primo (utilize o crivo de Eratóstenes, por exemplo). Portanto, o pequeno teorema de Fermat garante que $2^{996} \equiv 1 \pmod{997}$, de sorte que

$$2^{1992} = (2^{996})^2 \equiv 1 \pmod{997}.$$

A partir daí, é imediato que

$$f(1994) = 2^{1994} - 2 \equiv 2^2 - 2 \equiv 2 \pmod{997}.$$

Assim, temos o sistema linear de congruências

$$\begin{cases} f(1994) \equiv 0 \pmod 2 \\ f(1994) \equiv 2 \pmod{997} \end{cases},$$

o qual possui, pelo teorema chinês dos restos, uma única solução, módulo $2 \cdot 997 = 1994$. Mas, como 2 é claramente uma solução, segue que

$$f(1994) \equiv 2 \pmod{1994}.$$

□

Problemas – Seção 6.2

1. Prove que, para todo polinômio $f \in \mathbb{R}[X]$, temos

$$f(x+kh) = \sum_{j=0}^{k}\binom{k}{j}(\Delta_h^{k-j}f)(x),$$

para todos $h, x \in \mathbb{R}$ e todo $k \geq 0$.

2. (Canadá.) Seja f um polinômio de grau n, tal que $f(k) = \frac{k}{k+1}$ para todo inteiro $0 \leq k \leq n$. Calcule $f(n+1)$.

3. (Estados Unidos.) Seja f um polinômio de coeficientes reais e grau n, tal que $f(k) = \binom{n+1}{k}^{-1}$, para $0 \leq k \leq n$. Calcule os possíveis valores de $f(n+1)$.

4. Um polinômio f, de grau 990, é tal que $f(k) = F_k$ para $992 \leq k \leq 1982$, onde F_k é o $k-$ésimo número de Fibonacci. Prove que $f(1983) = F_{1983} - 1$.

5. Seja f um polinômio de coeficientes reais, tal que:

   (a) $f(1) > f(0) > 0$.

   (b) $f(2) > 2f(1) - f(0)$.

   (c) $f(3) > 3f(2) - 3f(1) + f(0)$.

   (d) $f(n+4) > 4f(n+3) - 6f(n+2) + 4f(n+1) - f(n)$ para todo $n \in \mathbb{N}$.

   Prove que $f(n) > 0$, para todo $n \in \mathbb{N}$.

CAPÍTULO 7

Fatoração de Polinômios

O algoritmo da divisão para polinômios fornece uma noção de divisibilidade em $\mathbb{K}[X]$ quando $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, a qual goza de propriedades análogas àquelas da noção correspondente para números inteiros. É, então, natural perguntar se, assim como em $\mathbb{Z}$, temos em $\mathbb{K}[X]$ polinômios *primos*, os quais forneçam algum tipo de *fatoração única*, com propriedades similares às da fatoração única de inteiros. Nosso propósito neste capítulo é fornecer respostas precisas a tais questões, as quais encompassarão também polinômios com coeficientes em $\mathbb{Z}_p$ (p primo). Referimos o leitor à introdução do capítulo 1 de [10] ou, mais geralmente, ao capítulo 1 de [14], para uma revisão dos conceitos correspondentes em $\mathbb{Z}$.

7.1 Fatoração única em $\mathbb{Q}[X]$

Ao longo desta seção, $\mathbb{K}$ denota $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Dizemos que dois polinômios $f, g \in \mathbb{K}[X] \setminus \{0\}$ são **associados** (em $\mathbb{K}[X]$) se existir $a \in \mathbb{K} \setminus \{0\}$ tal que $f = ag$. Por exemplo, os polinômios de coeficientes reais

$$f(X) = 4X^2 - 2X + 1 \text{ e } g(X) = 2\sqrt{2}X^2 - \sqrt{2}X + \frac{1}{\sqrt{2}}$$

são associados em $\mathbb{R}[X]$, uma vez que $f = \sqrt{2}g$ e $\sqrt{2} \in \mathbb{R} \setminus \{0\}$.

Se $f, g \in \mathbb{K}[X] \setminus \{0\}$ são dados, dizemos que um polinômio $p \in \mathbb{K}[X] \setminus \{0\}$ é um **divisor comum** de f e g quando $p \mid f, g$. Note que f e g sempre têm divisores comuns: os polinômios constantes e não nulos sobre $\mathbb{K}$, por exemplo.

Definição 7.1. *Dados $f, g \in \mathbb{K}[X]\setminus\{0\}$, dizemos que $d \in \mathbb{K}[X]\setminus\{0\}$ é um* **máximo divisor comum** *de f e g, e denotamos $d = \text{mdc}\,(f, g)$, se as duas condições a seguir forem satisfeitas:*

(a) $d \mid f, g$ em $\mathbb{K}[X]$.

(b) Se $d' \in \mathbb{K}[X] \setminus \{0\}$ divide f e g em $\mathbb{K}[X]$, então $d' \mid d$ em $\mathbb{K}[X]$.

O próximo resultado, também conhecido como o **teorema de Bézout**[1] para polinômios, garante a existência de um mdc para dois polinômios não nulos sobre $\mathbb{K}$, o qual é único a menos de associação (i.e., a menos de multiplicação por elementos não nulos de $\mathbb{K}$). Para o enunciado do mesmo, dado $f \in \mathbb{K}[X]$ denotamos por $f\mathbb{K}[X]$ o conjunto dos múltiplos de f em $\mathbb{K}[X]$, i.e.,

$$f\mathbb{K}[X] = \{af;\ a \in \mathbb{K}[X]\}.$$

Teorema 7.2. *Sejam $f, g \in \mathbb{K}[X] \setminus \{0\}$. Se*

$$S = \{af + bg;\ a, b \in \mathbb{K}[X]\},$$

então existe um polinômio $d \in \mathbb{K}[X] \setminus \{0\}$ satisfazendo as seguintes condições:

[1] Após 'Etienne Bézout, matemático francês do século XVIII.

(a) $S = d\mathbb{K}[X]$. Em particular, $d \mid f, g$ em $\mathbb{K}[X]$.

(b) Todo polinômio em $\mathbb{K}[X] \setminus \{0\}$ que divide f e g também divide d.

Ademais, tal polinômio d é único, a menos de associação.

Prova.
(a) Se $d \in S \setminus \{0\}$ é tal que

$$\partial d = \min\{\partial h;\ h \in S \setminus \{0\}\},$$

afirmamos inicialmente que $S = d\mathbb{K}[X]$. De fato, sendo $d = a_0 f + b_0 g$, com $a_0, b_0 \in \mathbb{K}[X]$, e $c \in \mathbb{K}[X]$, então

$$cd = (ca_0)f + (cb_0)g \in S,$$

i.e., $d\mathbb{K}[X] \subset S$. Reciprocamente, tome $h \in S$, digamos $h = af + bg$, com $a, b \in \mathbb{K}[X]$. Pelo algoritmo da divisão, temos $h = dq + r$, com $q, r \in \mathbb{K}[X]$ e $r = 0$ ou $0 \leq \partial r < \partial d$. Mas, se $r \neq 0$, então $\partial r < \partial d$ e

$$\begin{aligned} r &= h - dq = (af + bg) - (a_0 f + b_0 g)q \\ &= (a - a_0 q)f + (b - b_0 q)g \in S, \end{aligned}$$

uma contradição à minimalidade do grau de d em S. Logo, $r = 0$ e, daí, $h = dq \in d\mathbb{K}[X]$.

Para a segunda parte do item (a), basta ver que $f, g \in S = d\mathbb{K}[X]$, de forma que, em particular, f e g são múltiplos de d em $\mathbb{K}[X]$.

(b) Seja $d_1 \in \mathbb{K}[X] \setminus \{0\}$ um polinômio que divide f e g, digamos $f = d_1 f_1$ e $g = d_1 g_1$, com $f_1, g_1 \in \mathbb{K}[X]$. Se $a, b \in \mathbb{K}[X]$, então

$$af + bg = (af_1 + bg_1)d_1 \in d_1\mathbb{K}[X].$$

Mas, como $af + bg$ é um elemento genérico do conjunto S, segue então que

$$d \in d\mathbb{K}[X] = S \subset d_1\mathbb{K}[X];$$

em particular, d é um múltiplo de d_1, conforme desejado.

A última afirmação é deixada como exercício para o leitor (veja o problema 1). □

Graças à parte de unicidade do teorema de Bézout, doravante convencionamos que o mdc de dois polinômios não nulos sobre $\mathbb{K}$ é sempre mônico. Por outro lado, continuando a paráfrase com a noção de mdc em $\mathbb{Z}$, dizemos que dois polinômios $f, g \in \mathbb{K}[X] \setminus \{0\}$ são **primos entre si**, ou **relativamente primos**, quando $\text{mdc}\,(f, g) = 1$. Isto posto, temos a seguinte consequência do teorema anterior.

Corolário 7.3. *Se $f, g \in \mathbb{K}[X] \setminus \{0\}$, então f e g são primos entre si se, e só se, existem polinômios $a, b \in \mathbb{K}[X]$ tais que $af + bg = 1$.*

Prova. Se $\text{mdc}\,(f, g) = 1$, a existência de $a, b \in \mathbb{K}[X]$ como no enunciado segue do teorema de Bézout. Reciprocamente, se $d = \text{mdc}\,(f, g)$ e existem $a, b \in \mathbb{K}[X]$ tais que $af + bg = 1$, então, novamente pelo teorema de Bézout, temos que $1 \in d\mathbb{K}[X]$, i.e., d é um divisor do polinômio constante 1. Mas, uma vez que d é mônico, segue que $d = 1$. □

Corolário 7.4. *Sejam $f, g \in \mathbb{K}[X] \setminus \{0\}$ primos entre si e $h \in \mathbb{K}[X] \setminus \{0\}$ tal que $\partial h < \partial(fg)$. Então, existem $a, b \in \mathbb{K}[X]$ tais que $a = 0$ ou $\partial a < \partial g$, $b = 0$ ou $\partial b < \partial f$ e $af + bg = h$.*

Prova. Pelo corolário anterior, existem $a_1, b_1 \in \mathbb{K}[X]$ tais que $a_1 f + b_1 g = 1$. Daí, fazendo $a_2 = a_1 h$ e $b_2 = b_1 h$, temos $a_2 f + b_2 g = h$. Agora, pelo algoritmo da divisão, temos $a_2 = gq + a$, com $a = 0$ ou $0 \leq \partial a < \partial g$. Assim,

$$h = (gq + a)f + b_2 g = af + (qf + b_2)g$$

e, fazendo $b = qf + b_2$, temos $h = af + bg$, com $a = 0$ ou $\partial a < \partial g$. Por fim, como $bg = h - af$, se $b \neq 0$, temos

$$\partial b + \partial g = \partial(bg) = \partial(h - af) \leq \partial h < \partial(fg) = \partial f + \partial g,$$

de sorte que $\partial b < \partial f$. □

A definição a seguir é central para o restante deste capítulo.

Definição 7.5. *Um polinômio $p \in \mathbb{K}[X] \setminus \mathbb{K}$ é* **irredutível** *sobre $\mathbb{K}$ se p não puder ser escrito como produto de dois polinômios não constantes e com coeficientes em $\mathbb{K}$. Um polinômio $p \in \mathbb{K}[X] \setminus \mathbb{K}$ que não é irredutível é dito* **redutível** *sobre $\mathbb{K}$.*

Em geral, é útil refrasear a condição de irredutibilidade contrapositivamente; assim, um polinômio $p \in \mathbb{K}[X] \setminus \mathbb{K}$ é irredutível se, e só se, a seguinte condição for satisfeita:

$$p = gh, \text{ com } g, h \in \mathbb{K}[X] \Rightarrow g \in \mathbb{K} \text{ ou } h \in \mathbb{K}. \tag{7.1}$$

A fim de dar um sentido mais concreto ao conceito de polinômio irredutível, vejamos dois exemplos simples.

Exemplo 7.6. *É imediato, a partir de (7.1), que todo polinômio $p \in \mathbb{K}[X]$ de grau 1 é irredutível; de fato, sendo $p = gh$, com $g, h \in \mathbb{K}[X]$, segue da proposição 2.9 que $\partial g + \partial h = \partial p = 1$ e, daí, $\partial g = 0$ ou $\partial h = 0$, i.e., g ou h é constante. Por outro lado, pelo teorema fundamental da álgebra (o teorema 3.24), os polinômios irredutíveis em $\mathbb{C}[X]$ são precisamente aqueles de grau 1.*

Exemplo 7.7. *Se $p \in \mathbb{R}[X]$ é irredutível sobre $\mathbb{R}$, então $\partial p = 1$ ou 2. De fato, de acordo com o problema 2, página 74, um número complexo z é raiz de p se, e só se, $\overline{z}$ também o for. Consideremos, pois, dois casos separadamente:*

(a) $\partial p \geq 3$ e p tem pelo menos uma raiz real, α digamos: pelo teste da raiz (proposição 3.3) temos $p(X) = (X - \alpha)h(X)$, para algum $h \in \mathbb{R}[X]$ de grau 2, e p é redutível sobre $\mathbb{R}$.

(b) $\partial p \geq 3$ e p tem duas raízes não reais conjugadas, digamos z e $\overline{z}$: novamente pelo teste da raiz, temos $p(X) = (X-z)(X-\overline{z})h(X)$, para algum polinômio $h \in \mathbb{C}[X]$ de grau pelo menos 1. Mas, se $z = a+bi$ e $g(X) = (X-z)(X-\overline{z})$, então

$$g(X) = (X-a-bi)(X-a+bi) = (X-a)^2 + b^2 \in \mathbb{R}[X].$$

Portanto, aplicando o algoritmo da divisão à divisão de p por g, concluímos que $h \in \mathbb{R}[X]$. Assim, $p = gh$, com $g, h \in \mathbb{R}[X] \setminus \mathbb{R}$, e p é redutível sobre $\mathbb{R}$.

Graças ao exemplo acima, doravante consideraremos a noção de irredutibilidade de polinômios somente para polinômios sobre $\mathbb{Q}$. Nesse sentido, um argumento análogo ao do item (a) do último exemplo acima permite concluir que, se $p \in \mathbb{Q}[X]$ tem grau 2 ou 3, então p é irredutível sobre $\mathbb{Q}$ se, e só se, não tiver raízes em $\mathbb{Q}$ (veja o problema 3).

Voltando ao conceito geral de polinômio irredutível, note que, se $p \in \mathbb{Q}[X] \setminus \mathbb{Q}$ é irredutível, então os únicos divisores de p (em $\mathbb{Q}[X]$) são os polinômios constantes e aqueles associados a p. Temos, pois, o seguinte resultado importante.

Proposição 7.8. *Seja $p \in \mathbb{Q}[X]\setminus\mathbb{Q}$ irredutível. Se $f_1, \ldots, f_k \in \mathbb{Q}[X]\setminus\{0\}$ são tais que $p \mid f_1 \ldots f_k$, então existe $1 \leq i \leq k$ tal que $p \mid f_i$.*

Prova. Por indução, basta mostrarmos que, se $p \mid fg$, com $f, g \in \mathbb{Q}[X] \setminus \{0\}$, então $p \mid f$ ou $p \mid g$. Se $p \nmid f$, afirmamos inicialmente que $\mathrm{mdc}\,(f,p) = 1$; de fato, se $d = \mathrm{mdc}\,(f,p)$, então $d \mid p$, de forma que $d \in \mathbb{Q}$ ou d é associado a p em $\mathbb{Q}[X]$. Mas, se d for associado a p, então segue de $d \mid f$ que $p \mid f$, o que é uma contradição. Logo, $d \in \mathbb{Q}$ e, daí, $d = 1$.

Agora, pelo corolário 7.3, existem polinomios $a, b \in \mathbb{Q}[X]$ tais que $af + bp = 1$, de sorte que

$$a(fg) + (bg)p = g.$$

Como $p \mid (fg)$, segue da igualdade acima e do problema 4 que $p \mid g$, conforme desejado. □

No que segue, mostraremos que todo polinômio $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ pode ser escrito unicamente, a menos de associação, como o produto de um número finito de polinômios irredutíveis. Mais precisamente, mostraremos que:

(i) Existem polinômios irredutíveis $p_1, \ldots, p_k \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tais que $f = p_1 \ldots p_k$.

(ii) Se $q_1, \ldots, q_l \in \mathbb{Q}[X] \setminus \mathbb{Q}$ são também irredutíveis e tais que $f = q_1 \ldots q_l$, então $k = l$ e, a menos de uma reordenação, p_i e q_i são associados em $\mathbb{Q}[X]$.

Comecemos examinando a parte de existência.

Proposição 7.9. *Todo polinômio $f \in \mathbb{Q}[X]\setminus\mathbb{Q}$ pode ser escrito como produto de um número finito de polinômios irredutíveis sobre $\mathbb{Q}$.*

Prova. Façamos indução sobre ∂f, sendo o caso $\partial f = 1$ imediato (já vimos que, nesse caso, f é irredutível). Por hipótese de indução, suponha o resultado verdadeiro para todo polinômio em $\mathbb{Q}[X] \setminus \mathbb{Q}$ de grau menor que n, e tome $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tal que $\partial f = n$. Se f for irredutível, nada há a fazer. Senão, podemos escrever $f = gh$, com $g, h \in \mathbb{Q}[X]\setminus\mathbb{Q}$. Logo, $\partial g, \partial h < n$, e a hipótese de indução garante que g e h podem ambos ser escritos como produtos de um número finito de polinômios irredutíveis sobre $\mathbb{Q}$, digamos $g = p_1 \ldots p_j$ e $h = p_{j+1} \ldots p_k$. Então $f = gh = p_1 \ldots p_j p_{j+1} \ldots p_k$, um produto finito de polinômios irredutíveis sobre $\mathbb{Q}$. □

O próximo resultado garante a validade da parte de unicidade (a menos de associação) da representação de um polinômio não constante sobre $\mathbb{Q}$ como produto de polinômios irredutíveis.

Proposição 7.10. *Se $p_1, \ldots, p_k, q_1, \ldots, q_l \in \mathbb{Q}[X] \setminus \mathbb{Q}$ são irredutíveis e tais que $p_1 \ldots p_k = q_1 \ldots q_l$, então $k = l$ e, a menos de uma reordenação, p_i e q_i são associados sobre $\mathbb{Q}$.*

Prova. Se $k = 1$, temos $p_1 = q_1 \ldots q_l$, e a irredutibilidade de p_1 garante que $l = 1$. Analogamente, $l = 1 \Rightarrow k = 1$. Suponha, pois, $k, l > 1$; como $p_k \mid q_1 \ldots q_l$, a proposição 7.8 garante a existência de $1 \leq j \leq l$ tal que $p_k \mid q_j$. Suponha, sem perda de generalidade, $j = l$. Como q_l é irredutível e $p_k \notin \mathbb{Q}$, a única possibilidade é que p_k e q_l sejam associados, digamos $p_k = uq_l$, com $u \in \mathbb{Q} \setminus \{0\}$. Então

$$p_1 \ldots p_{k-1} = q_1 \ldots q_{l-2} u q_{l-1} = q_1' \ldots q_{l-1}',$$

com $q_i' = q_i$ para $1 \leq i < l - 2$ e $q_{l-1}' = uq_{l-1}$, todos irredutíveis sobre $\mathbb{Q}$.

Por indução sobre $\max\{k, l\}$, temos $k - 1 = l - 1$ e, a menos de uma reordenação, p_i associado a q_i' para $1 \leq i \leq l - 1$. Portanto, a menos de uma reordenação, p_i e q_i são também associados sobre $\mathbb{Q}$. □

Resumimos as duas proposições acima dizendo que, em $\mathbb{Q}[X]$, temos *fatoração única*. Assim como em $\mathbb{Z}$, se $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ é tal que

$$f = p_1 \ldots p_k,$$

com $p_1, \ldots, p_k \in \mathbb{Q}[X] \setminus \mathbb{Q}$ irredutíveis, então, reunindo os fatores p_i iguais a menos de associação, obtemos

$$f = q_1^{\alpha_1} \ldots q_l^{\alpha_1}, \tag{7.2}$$

com $q_1, \ldots, q_l \in \mathbb{Q}[X] \setminus \mathbb{Q}$ irredutíveis e dois a dois não associados, e α_1, $\ldots$, $\alpha_l \in \mathbb{N}$. A expressão (7.2) (também única a menos de associação) é a **fatoração canônica** de f em $\mathbb{Q}[X]$, e $q_1, \ldots, q_l$ são os **fatores irredutíveis** de f em $\mathbb{Q}[X]$.

Problemas – Seção 7.1

1. * Complete a prova do teorema 7.2.

2. Sejam $f, g \in \mathbb{Q}[X] \setminus \mathbb{Q}$ polinômios tais que
$$f = p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\alpha_1'} \ldots q_l^{\alpha_l'} \text{ e } g = p_1^{\beta_1} \ldots p_k^{\beta_k} r_1^{\beta_1'} \ldots r_m^{\beta_m'},$$
onde $p_1, \ldots, p_k$, $q_1, \ldots, q_l$ e $r_1, \ldots, r_m$ são polinômios mônicos e irredutíveis, dois a dois não associados, e α_i, α_i', β_j, $\beta_j' \in \mathbb{N}$. Prove que
$$\text{mdc}\,(f, g) = p_1^{\gamma_1} \ldots p_k^{\gamma_k},$$
com $\gamma_i = \min\{\alpha_i, \beta_i\}$, para $1 \leq i \leq k$.

3. * Se $p \in \mathbb{Q}[X]$ é um polinômio de grau 2 ou 3, prove que p é irredutível sobre $\mathbb{Q}$ se, e só se, p não tiver raízes em $\mathbb{Q}$.

4. * Se $f, g, h \in \mathbb{Q}[X] \setminus \{0\}$ são tais que $f \mid g, h$, prove que f divide $ag + bh$, para todos $a, b \in \mathbb{Q}[X]$.

5. Se $f \in \mathbb{R}[X] \setminus \mathbb{R}$ tem grau maior que 1, prove que f pode ser escrito, de maneira única a menos de associação, como produto de um número finito de polinômios irredutíveis sobre $\mathbb{R}$.

6. O objetivo deste problema é estabelecer a existência de decomposições de quocientes de polinômios em frações parciais. Para tanto, sejam dados $f, g \in \mathbb{K}[X] \setminus \{0\}$.

   (a) Se $\partial f < \partial g$ e $g = g_1^{\alpha_1} \ldots g_k^{\alpha_k}$ é a fatoração canônica de g em polinômios irredutíveis de $\mathbb{K}[X]$, prove que existem polinômios f_1, $\ldots$, f_k em $\mathbb{K}[X]$, tais que $f_j = 0$ ou $\partial f_j < \partial(g_j^{\alpha_j})$, para $1 \leq j \leq k$, e
   $$\frac{f}{g} = \sum_{j=1}^{k} \frac{f_j}{g_j^{\alpha_j}}.$$

(b) Se g é irredutível sobre $\mathbb{K}$ e $k \geq 1$ é inteiro, prove que existem polinômios $q, r_1, \ldots, r_k \in \mathbb{K}[X]$, com $r_j = 0$ ou $\partial r_j < \partial g$, tais que

$$\frac{f}{g^k} = q + \sum_{j=1}^{k} \frac{r_j}{g^j}.$$

7.2 Fatoração única em $\mathbb{Z}[X]$

Estudamos, na seção anterior, o problema de fatoração única para polinômios com coeficientes racionais. Nesta seção, estendemos a análise de tal problema a polinômios com coeficientes inteiros. Nesse sentido, a definição a seguir se revelará crucial.

Definição 7.11. *Se $f \in \mathbb{Z}[X] \setminus \{0\}$, o* **conteúdo** *$c(f)$ de f é o* mdc *de seus coeficientes não nulos. Se $c(f) = 1$, dizemos que f é um polinômio* **primitivo** *em $\mathbb{Z}[X]$.*

Por simplicidade de notação, se $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X] \setminus \{0\}$, denotamos

$$c(f) = \text{mdc}\,(a_0, \ldots, a_n).$$

O lema a seguir, cuja prova deixamos ao leitor (veja o problema 1), estabelece duas propriedades úteis do conceito de conteúdo de um polinômio de coeficientes inteiros.

Lema 7.12.

(a) Se $f \in \mathbb{Z}[X] \setminus \{0\}$ e $a \in \mathbb{Z} \setminus \{0\}$, então $c(af) = |a| \cdot c(f)$. Em particular, existe $g \in \mathbb{Z}[X] \setminus \{0\}$ primitivo tal que $f = c(f)g$.

(b) Se $f \in \mathbb{Q}[X] \setminus \{0\}$, então, a menos de multiplicação por -1, existem únicos $a, b \in \mathbb{Z}\setminus\{0\}$ primos entre si e $g \in \mathbb{Z}[X]$ primitivo tais que $f = (a/b)g$.

A importância do conceito de conteúdo de um polinômio de coeficientes inteiros reside no papel chave que o mesmo desempenha no estudo de polinômios irredutíveis sobre $\mathbb{Z}$, a começar pela definição dos mesmos.

Definição 7.13. [2] *Um polinômio $p \in \mathbb{Z}[X] \setminus \mathbb{Z}$ é* **irredutível** *sobre $\mathbb{Z}$ se p for primitivo e não puder ser escrito como produto de dois polinômios não constantes em $\mathbb{Z}[X]$. Um polinômio primitivo $p \in \mathbb{Z}[X] \setminus \mathbb{Z}$ que não é irredutível é dito* **redutível** *sobre $\mathbb{Z}$.*

Novamente, é útil refrasear a condição de irredutibilidade de polinômios de coeficientes inteiros contrapositivamente, de modo que um polinômio primitivo $p \in \mathbb{Z}[X] \setminus \mathbb{Z}$ é irredutível se, e só se, a seguinte condição for satisfeita:

$$p = gh, \text{ com } g, h \in \mathbb{Z}[X] \Rightarrow g = \pm 1 \text{ ou } h = \pm 1. \tag{7.3}$$

A proposição a seguir é conhecida como o **lema de Gauss**.

Proposição 7.14 (Gauss). *Para $f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$, temos que:*

(a) $c(fg) = c(f)c(g)$. Em particular, fg é primitivo se, e só se, f e g o forem[3].

(b) Se f é primitivo, então f é irredutível em $\mathbb{Z}[X]$ se, e só se, o for em $\mathbb{Q}[X]$.

(c) Se f e g forem primitivos e associados em $\mathbb{Q}[X]$, então $f = \pm g$.

Prova.
(a) Pelo lema 7.12, se $f = c(f)f_1$ e $g = c(g)g_1$, então $f_1, g_1 \in \mathbb{Z}[X]$ são primitivos e $fg = c(f)c(g)f_1g_1$, de modo que $c(fg) = c(f)c(g)c(f_1g_1)$.

[2]Apesar da definição que adotamos aqui para polinômios em $\mathbb{Z}[X]$ irredutíveis ser ligeiramente mais restritiva que a usualmente encontrada na literatura (conforme [28], por exemplo), ela será suficiente para nossos propósitos.

[3]Para uma outra prova, veja o problema 7, página 178.

Portanto, basta mostrarmos que f_1g_1 é primitivo, ou, o que é o mesmo, que

$$f, g \text{ primitivos} \Leftrightarrow fg \text{ primitivo}.$$

Se f não for primitivo, existe $p \in \mathbb{Z}$ primo tal que p divide todos os coeficientes de f. Então, p divide todos os coeficientes de fg, e fg não é primitivo. Analogamente, se g não for primitivo, então fg também não é primitivo.

Reciprocamente, suponha que $f(X) = a_mX^m + \cdots + a_1X + a_0$ e $g(X) = b_nX^n + \cdots + b_1X + b_0$ são primitivos mas fg não o é. Tome $p \in \mathbb{Z}$ primo tal que p divide todos os coeficientes de fg, e sejam $k, l \geq 0$ os menores índices tais que $p \nmid a_k, b_l$ (tais k e l existem, uma vez que f e g são primitivos). Denotando por c_{k+l} o coeficiente de X^{k+l} em fg, segue que

$$c_{k+l} = \cdots + a_{k-2}b_{l+2} + a_{k-1}b_{l+1} + a_kb_l + a_{k+1}b_{l-1} + a_{k+2}b_{l-2} + \cdots.$$

Agora, como $p \mid c_{k+l}$ e $p \mid a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}$, a igualdade acima garante que $p \mid a_kb_l$, o que é uma contradição.

(b) A implicação $\Leftarrow$) é clara. Reciprocamente, tome $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ primitivo e suponha que f é redutível em $\mathbb{Q}[X]$, digamos $f = gh$, com $g, h \in \mathbb{Q}[X]\setminus\mathbb{Q}$. Pelo lema 7.12, podemos tomar $a, b, c, d \in \mathbb{Z}\setminus\{0\}$ tais que $g = (a/b)g_1$ e $h = (c/d)h_1$, com $g_1, h_1 \in \mathbb{Z}[X]$ primitivos. Então,

$$bdf = bg \cdot dh = ag_1 \cdot ch_1 = acg_1h_1.$$

Mas, como g_1h_1 é primitivo pelo item (a), tomando conteúdos na igualdade acima obtemos $|bd| \cdot c(f) = |ac|$. Logo, $\frac{ac}{bd} = \pm c(f) \in \mathbb{Z}$, e segue novamente da igualdade acima que $f = \pm c(f)g_1h_1$, i.e., f é redutível em $\mathbb{Z}[X]$.

(c) Se $f = (a/b)g$, com $a, b \in \mathbb{Z} \setminus \{0\}$, então $bf = ag$ e, tomando conteúdos, obtemos $|b| \cdot c(f) = |a| \cdot c(g)$. Mas, uma vez que $c(f) = 1$ e $c(g) = 1$, segue que $|a| = |b|$, de sorte que $a/b = \pm 1$. □

Podemos, finalmente, enunciar e provar um celebrado resultado de Gauss, o qual se constitui, para polinômios de coeficientes inteiros, no análogo das proposições 7.9 e 7.10.

Teorema 7.15 (Gauss). *Todo polinômio primitivo $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ pode ser escrito como produto de um número finito de polinômios irredutíveis em $\mathbb{Z}[X]$. Ademais, tal maneira de escrever f é única a menos de uma reordenação dos fatores e de multiplicação de alguns dos mesmos por -1.*

Prova. Mostremos primeiramente a existência da fatoração em irredutíveis: vendo f como polinômio em $\mathbb{Q}[X]$, segue da proposição 7.9 a existência de polinômios irredutíveis $p_1, \ldots, p_k \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tais que $f = p_1 \ldots p_k$. Escreva $p_i = (a_i/b_i)q_i$, com $a_i, b_i \in \mathbb{Z}\setminus\{0\}$ relativamente primos e $q_i \in \mathbb{Z}[X] \setminus \mathbb{Z}$ primitivo. Como q_i também é obviamente irredutível em $\mathbb{Q}[X]$, segue do item (b) do lema de Gauss que q_i é irredutível em $\mathbb{Z}[X]$. Sendo $a = a_1 \ldots a_k$ e $b = b_1 \ldots b_k$, temos então que

$$f = (a/b)q_1 \ldots q_k.$$

Mas, como $q_1, \ldots, q_k$ são todos primitivos, o item (a) do lema de Gauss garante que $q_1 \ldots q_k$ também é primitivo. Assim, tomando conteúdos na igualdade acima, obtemos

$$|b| = |b| \cdot c(f) = |a| \cdot c(q_1 \ldots q_k) = |a|.$$

Portanto, segue que $a/b = \pm 1$ e, daí, $f = q_1 \ldots q_k$, um produto de polinômios irredutíveis de $\mathbb{Z}[X]$.

A prova da parte de unicidade do enunciado é essencialmente idêntica à prova da proposição 7.10, uma vez que provemos o seguinte: se $p, f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$ são tais que p é irredutível e $p \mid fg$ em $\mathbb{Z}[X]$, então $p \mid f$ ou $p \mid g$ em $\mathbb{Z}[X]$. Para tanto, note inicialmente (novamente pelo item (b) do lema de Gauss) que p também é irredutível em $\mathbb{Q}[X]$ e, assim sendo, já sabemos que $p \mid f$ ou $p \mid g$ em $\mathbb{Q}[X]$. Se $p \mid f$ em $\mathbb{Q}[X]$

(o outro caso é análogo), existe $f_1 \in \mathbb{Q}[X]$ tal que $f = f_1 p$. Tomando $a, b \in \mathbb{Z}$ tais que $f_1 = (a/b) f_2$, com $f_2 \in \mathbb{Z}[X] \setminus \mathbb{Z}$ primitivo, temos

$$bf = bf_1 p = af_2 p.$$

Agora, p e f_2 primitivos implica (uma vez mais pelo item (a) do lema de Gauss) em $f_2 p$ primitivo e, tomando conteúdos na igualdade acima, obtemos $|b| \cdot c(f) = |a| \cdot c(f_2 p) = |a|$. Portanto, $a/b = \pm c(f) \in \mathbb{Z}$, de maneira que $f_1 \in \mathbb{Z}[X]$ e $p \mid f$ em $\mathbb{Z}[X]$. □

Problemas – Seção 7.2

1. * Prove o lema 7.12.

2. * Seja $f \in \mathbb{Z}[X]$ um polinômio mônico e não constante. Se f é redutível sobre $\mathbb{Q}$, prove que existem polinômios mônicos e não constantes $g, h \in \mathbb{Z}[X]$, tais que $f = gh$.

7.3 Polinômios sobre $\mathbb{Z}_p$

Vimos, à seção 6.2 de [14], que, para p primo, o conjunto $\mathbb{Z}_p$ das classes de congruência módulo p pode ser munido com operações de adição, subtração, multiplicação e divisão bastante similares às suas análogas em $\mathbb{C}$. Tal semelhança faz com que praticamente todos os conceitos e resultados sobre polinômios estudados até o momento continuem válidos no conjunto $\mathbb{Z}_p[X]$ dos polinômios com coeficientes em $\mathbb{Z}_p$.

Nosso propósito aqui é comentar explicitamente algumas semelhanças e diferenças entre polinômios sobre $\mathbb{Z}_p$ e sobre $\mathbb{K}$, com $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, deixando ao leitor a tarefa de checar que todos os demais resultados e definições para $\mathbb{K}[X]$ apresentados no texto (exceto por

aqueles das seções 3.3 e 6.2 e do capítulo 5) são válidos *ipsis literis* para $\mathbb{Z}_p[X]$. Aproveitamos também para deduzir, com o auxílio de polinômios sobre $\mathbb{Z}_p$, alguns resultados de teoria dos números e combinatória não acessíveis pelos métodos de que dispomos até o presente momento. Em particular, demonstramos a existência de raízes primitivas módulo p, completando, assim, a discussão da seção 7.2 de [14].

Dado $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, denote por $\overline{f} \in \mathbb{Z}_p[X]$ o polinômio

$$\overline{f}(X) = \overline{a}_n X^n + \cdots + \overline{a}_1 X + \overline{a}_0, \tag{7.4}$$

onde $\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_n$ denotam, respectivamente, as classes de congruência de a_0, a_1, ..., a_n, módulo p.

A correspondência $f \mapsto \overline{f}$ define uma aplicação

$$\begin{array}{rccc} \pi_p : & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_p[X] \\ & f & \longmapsto & \overline{f} \end{array},$$

a qual é obviamente sobrejetiva, sendo denominada a **projeção** de $\mathbb{Z}[X]$ sobre $\mathbb{Z}_p[X]$. Para $f, g \in \mathbb{Z}[X]$, é imediato verificar que

$$\begin{gathered} \overline{f}(X) = \overline{g}(X) \text{ em } \mathbb{Z}_p[X] \\ \Updownarrow \\ \exists h \in \mathbb{Z}[X];\ f(X) = g(X) + ph(X) \text{ em } \mathbb{Z}[X]. \end{gathered}$$

Equivalentemente, denotando

$$p\mathbb{Z}[X] = \{ph;\ h \in \mathbb{Z}[X]\},$$

temos

$$\overline{f} = \overline{0} \Leftrightarrow f \in p\mathbb{Z}[X].$$

Estendemos as operações de adição e multiplicação de $\mathbb{Z}_p$ a operações homônimas $+, \cdot : \mathbb{Z}_p[X] \times \mathbb{Z}_p[X] \to \mathbb{Z}_p[X]$ pondo, para $f, g \in \mathbb{Z}[X]$,

$$\overline{f} + \overline{g} = \overline{f + g} \text{ e } \overline{f} \cdot \overline{g} = \overline{fg}.$$

Deixamos a cargo do leitor a verificação da boa definição da adição e da multiplicação de $\mathbb{Z}_p[X]$, a qual pode ser feita de maneira análoga à verificação da boa definição das operações de $\mathbb{Z}_p$ (de acordo com a seção 6.2 de [14]; veja também o problema 1, página 177).

Assim como em $\mathbb{Z}[X]$, dizemos que um polinômio $\overline{f} \in \mathbb{Z}_p[X] \setminus \{\overline{0}\}$ como em (7.4) tem grau n se $\overline{a}_n \neq \overline{0}$, i.e., se $p \nmid a_n$. Mais geralmente, se $f \in \mathbb{Z}[X] \setminus p\mathbb{Z}[X]$, então $\overline{f} \neq \overline{0}$ e $\partial \overline{f} \leq \partial f$.

Os dois exemplos a seguir utilizam a multiplicação de polinômios em $\mathbb{Z}_p[X]$ para provar propriedades interessantes de números binomiais.

Exemplo 7.16. *Se p é um número primo e k é um inteiro positivo, prove que $\binom{p^k}{j}$ é múltiplo de p, para $1 \leq j < p^k$.*

Prova. Pelo exemplo 1.41 de [14], já sabemos que $(X+\overline{1})^p = X^p + \overline{1}$ em $\mathbb{Z}_p[X]$. Por hipótese de indução, suponha que, para algum $l \in \mathbb{N}$, tenhamos provado que

$$(X+\overline{1})^{p^l} = X^{p^l} + \overline{1}$$

em $\mathbb{Z}_p[X]$. Então, aplicando sucessivamente o caso inicial e a hipótese de indução, obtemos

$$(X+\overline{1})^{p^{l+1}} = (X^p+\overline{1})^{p^l} = (X^p)^{p^l} + \overline{1} = X^{p^{l+1}} + \overline{1}.$$

Por outro lado, também temos

$$(X+\overline{1})^{p^k} = X^{p^k} + \overline{\binom{p^k}{p^k-1}} X^{p^k-1} + \cdots + \overline{\binom{p^k}{1}} X + \overline{1},$$

de modo que, para $1 \leq j < p^k$, temos $\overline{\binom{p^k}{j}} = \overline{0}$; daí, p divide o número binomial $\binom{p^k}{j}$. □

Exemplo 7.17 (Romênia). *Prove que o número de coeficientes binomiais ímpares na $n-$ésima linha do triângulo de Pascal é uma potência de 2.*

Prova. Seja (de acordo com o exemplo 5.12 de [10])

$$n = 2^{a_k} + 2^{a_{k-1}} + \cdots + 2^{a_1} + 2^{a_0}$$

a representação binária de n, onde $0 \leq a_0 < a_1 < \cdots < a_k$. Pelo exemplo 7.16, temos em $\mathbb{Z}_2[X]$ que

$$\begin{aligned}(X+\overline{1})^n &= (X+\overline{1})^{2^{a_k}}(X+\overline{1})^{2^{a_{k-1}}}\ldots(X+\overline{1})^{2^{a_0}} \\ &= (X^{2^{a_k}}+\overline{1})(X^{2^{a_{k-1}}}+\overline{1})\ldots(X^{2^{a_0}}+\overline{1}).\end{aligned} \tag{7.5}$$

Sendo S o conjunto dos números formados a partir de somas de potências distintas de 2, escolhidas dentre as potências 2^{a_k}, $2^{a_{k-1}}$, ..., 2^{a_1} e 2^{a_0}, temos pelo princípio fundamental da contagem e pela unicidade da representação binária de naturais, que $|S| = 2^{k+1}$; por outro lado, efetuando os produtos da última expressão de (7.5), obtemos

$$(X+\overline{1})^n = \sum_{m \in S} X^m, \tag{7.6}$$

uma soma com exatamente 2^{k+1} parcelas. Mas, uma vez que a fórmula de expansão binomial fornece

$$(X+\overline{1})^n = X^n + \overline{\binom{n}{1}} X^{n-1} + \cdots + \overline{\binom{n}{n-1}} X + \overline{1}, \tag{7.7}$$

comparando as expressões (7.6) e (7.7), concluímos que exatamente 2^{k+1} dentre os números binomiais da forma $\binom{n}{j}$ (os quais compõem a $n-$ésima linha do triângulo de Pascal) são tais que $\overline{\binom{n}{j}} \neq \overline{0}$, i.e., são ímpares. □

Para definir a função polinomial associada a um polinômio $\overline{f} \in \mathbb{Z}_p[X]$ temos que ter alguns cuidados. Note inicialmente que, se $f \in \mathbb{Z}[X]$ e $a, b \in \mathbb{Z}$ são tais que $a \equiv b \pmod p$, então o item (c) da proposição 5.6 de [14] garante que

$$f(a) \equiv f(b) \pmod p;$$

por outro lado, se $\overline{f} = \overline{g}$ em $\mathbb{Z}_p[X]$, vimos acima que existe $h \in \mathbb{Z}[X]$ tal que $f(X) = g(X) + ph(X)$. Portanto, para $a \in \mathbb{Z}$, temos

$$f(a) = g(a) + ph(a) \equiv g(a) \pmod{p}.$$

Dado $\overline{f} \in \mathbb{Z}_p[X]$, os comentários acima permitem definir a função polinomial associada $\tilde{f} : \mathbb{Z}_p \to \mathbb{Z}_p$ pondo, para $a \in \mathbb{Z}$,

$$\tilde{f}(\overline{a}) = \overline{g(a)}, \tag{7.8}$$

onde $g \in \mathbb{Z}[X]$ é qualquer polinômio tal que $\overline{f} = \overline{g}$. Obviamente, a imagem de $\tilde{f}$ é um conjunto finito, uma vez que o próprio $\mathbb{Z}_p$ o é. Doravante, sempre que não houver perigo de confusão, escreveremos (7.8) simplesmente como

$$\overline{f}(\overline{a}) = \overline{f(a)}.$$

O exemplo a seguir mostra que, contrariamente ao que ocorre com polinômios sobre $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, a função polinomial associada a um polinômio não nulo em $\mathbb{Z}_p[X]$ pode ser identicamente nula. Em particular, *não é mais válido* que dois polinômios sobre $\mathbb{Z}_p$ só terão funções polinomiais iguais quando forem eles mesmos iguais.

Exemplo 7.18. *O polinômio $f(X) = X^p - X \in \mathbb{Z}_p[X]$ é claramente um elemento não nulo de $\mathbb{Z}_p[X]$. Por outro lado, denotando por $\overline{f}$: $\mathbb{Z}_p \to \mathbb{Z}_p$ a função polinomial associada ao mesmo, temos pelo pequeno teorema de Fermat (veja [14]) que*

$$\overline{f}(\overline{a}) = \overline{a}^p - \overline{a} = \overline{a^p - a} = \overline{0},$$

para todo $\overline{a} \in \mathbb{Z}_p$. Assim, $\overline{f}$ é a função identicamente nula.

Sejam dados $f \in \mathbb{Z}[X]$ e $a \in \mathbb{Z}$. Como na seção 3.1, dizemos que $\overline{a} \in \mathbb{Z}_p$ é uma raiz de $\overline{f}$ se $\overline{f}(\overline{a}) = \overline{0}$. Uma rápida inspeção da prova do teste da raiz mostra que o mesmo continua válido em $\mathbb{Z}_p[X]$. Em particular, obtemos, a partir do exemplo acima, o seguinte resultado importante.

Proposição 7.19. *Em $\mathbb{Z}_p[X]$, temos*

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2}) \ldots (X - \overline{(p-1)}).$$

Prova. Como $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ são raízes de $X^{p-1} - \overline{1}$ em $\mathbb{Z}_p$ (novamente pelo pequeno teorema de Fermat), o item (c) da proposição 3.3 garante que $X^{p-1} - \overline{1}$ é divisível em $\mathbb{Z}_p[X]$ pelo polinômio $(X - \overline{1})(X - \overline{2}) \ldots (X - \overline{(p-1)})$. Mas, como ambos tais polinômios são mônicos e têm grau $p - 1$, segue que

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2}) \ldots (X - \overline{(p-1)}).$$

□

Em $\mathbb{Z}_p[X]$, as definições e resultados da seção 7.1 mantém-se completamente. Em particular, podemos enunciar o seguinte teorema, cuja prova é totalmente análoga às provas das proposições 7.9 e 7.10.

Teorema 7.20. *Se $p \in \mathbb{Z}$ é primo, então todo polinômio $\overline{f} \in \mathbb{Z}_p[X] \setminus \mathbb{Z}_p$ pode ser escrito, de maneira única a menos de reordenação e associação, como produto de um número finito de polinômios irredutíveis sobre $\mathbb{Z}_p[X]$.*

Como primeira aplicação do resultado acima, provamos, a seguir, a existência de raízes primitivas módulo p.[4] Para o enunciado e prova do mesmo, sugerimos ao leitor rever o material da seção 7.2 de [14].

Teorema 7.21. *Se p é um primo ímpar e d é um divisor positivo de $p - 1$, então a congruência*

$$x^{p-1} - 1 \equiv 0 \pmod{p} \tag{7.9}$$

tem exatamente $\varphi(d)$ raízes de ordem d, duas a duas incongruentes módulo p. Em particular, p possui raízes primitivas.

[4]Para comodidade do leitor, recordamos que um inteiro a, não divisível por um primo p, é denominado uma *raiz primitiva* módulo p se $p - 1$ for o menor inteiro positivo k satisfazendo a congruência $a^k \equiv 1 \pmod{p}$.

Prova. Para d divisor positivo de $p-1$, seja $N(d)$ o número de raízes da congruência (7.9), com ordem d e duas a duas incongruentes, módulo p. Uma vez que as raízes da congruência (7.9) são os inteiros $1, 2, \ldots, p-1$ e (pela proposição 7.2 de [14]) cada um de tais números tem ordem igual a um divisor de $p-1$, concluímos que

$$\sum_{0<d|(p-1)} N(d) = p-1.$$

Portanto, se mostrarmos que $N(d) \leq \varphi(d)$, seguirá da proposição 3.11 de [14] que

$$p-1 = \sum_{0<d|(p-1)} N(d) \leq \sum_{0<d|(p-1)} \varphi(d) = p-1$$

e, daí, que $N(d) = \varphi(d)$, para todo divisor positivo d de $p-1$.

Seja, então, d um divisor positivo de $p-1$. Se $N(d) = 0$, é claro que $N(d) \leq \varphi(d)$. Senão, seja a um inteiro de ordem d, módulo p; então, as classes $\overline{1}$, $\overline{a}$, $\ldots$, $\overline{a}^{d-1} \in \mathbb{Z}_p$ são raízes duas a duas distintas do polinômio $X^d - \overline{1} \in \mathbb{Z}_p[X]$. Por outro lado, o corolário 3.8 garante que tal polinômio possui no máximo d raízes em $\mathbb{Z}_p$, de sorte que suas raízes são exatamente $\overline{1}$, $\overline{a}$, $\ldots$, $\overline{a}^{d-1}$. Portanto, se $\alpha \in \mathbb{Z}$ for uma raiz de ordem d de (7.9), então $\overline{\alpha} \in \mathbb{Z}_p$ é raiz de $X^d - \overline{1} \in \mathbb{Z}_p[X]$, de sorte que $\overline{\alpha} \in \{\overline{1}, \overline{a}, \ldots, \overline{a}^{d-1}\}$. Assim, as raízes de ordem d de (7.9) são exatamente os elementos de ordem d do conjunto $\{1, a, \ldots, a^{d-1}\}$ e, daí,

$$N(d) = \#\{0 \leq k \leq d-1;\ \mathrm{ord}_p(a^k) = d\}.$$

O item (c) da proposição 7.5 de [14] conta o número de elementos do segundo membro acima: como $\mathrm{ord}_p(a) = d$, temos

$$\mathrm{ord}_p(a^k) = d \Leftrightarrow \frac{d}{\mathrm{mdc}\,(d,k)} = d \Leftrightarrow \mathrm{mdc}\,(d,k) = 1;$$

portanto,

$$\begin{aligned} &\#\{0 \leq k \leq d-1;\ \mathrm{ord}_p(a^k) = d\} = \\ &= \#\{0 \leq k \leq d-1;\ \mathrm{mdc}\,(d,k) = 1\} \\ &= \varphi(d). \end{aligned}$$

Assim, $N(d) = 0$ ou $\varphi(d)$ e, em qualquer caso, temos $N(d) \leq \varphi(d)$, conforme desejado.

Para o que falta, basta notar que $N(p-1) = \varphi(p-1)$, ou seja, há exatamente $\varphi(p-1)$ inteiros, dois a dois incongruentes, módulo p, e com ordem $p-1 = \varphi(p)$, módulo p; de outro modo, há exatamente $\varphi(p-1)$ raízes primitivas, módulo p, duas a duas incongruentes, módulo p (veja que este resultado concorda com a proposição 7.8 de [14]). □

Terminamos esta seção exibindo mais uma aplicação da teoria de polinômios sobre $\mathbb{Z}_p$ à Teoria dos Números.

Exemplo 7.22 (Miklós-Schweitzer). *Se $p > 3$ é um primo tal que $p \equiv 3\,(\mathrm{mod}\,4)$, prove que*

$$\prod_{1 \leq x \neq y \leq \frac{p-1}{2}} (x^2 + y^2) \equiv 1\,(\mathrm{mod}\,p).$$

Prova. Em tudo o que segue, salvo menção em contrário os índices dos produtórios apresentados variam de 1 a $\frac{p-1}{2}$.

Se P denota o produto do primeiro membro, então

$$\begin{aligned} P &= \prod_{x \neq 1}(x^2 + 1^2) \cdot \prod_{x \neq 2}(x^2 + 2^2) \cdots \prod_{x \neq \frac{p-1}{2}} \left(x^2 + \left(\frac{p-1}{2}^2\right)\right) \\ &= \frac{\prod(x^2+1^2) \cdot \prod(x^2+2^2) \cdots \prod\left(x^2 + \left(\frac{p-1}{2}^2\right)\right)}{2^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2}. \end{aligned}$$

Agora, para $1 \leq k \leq \frac{p-1}{2}$, denote por c_k o inverso de k, módulo p. Módulo p, tem-se

$$\prod(x^2 + k^2) \equiv k^2 \prod((c_k x)^2 + 1) \equiv k^2 \prod(x^2 + 1).$$

De fato, a primeira congruência é imediata e, para a segunda, basta observar que $\{(c_k x)^2;\ 1 \leq x \leq \frac{p-1}{2}\}$ é um conjunto de $\frac{p-1}{2}$ resíduos quadráticos dois a dois incongruentes, módulo p; portanto, $\{(c_k x)^2;\ 1 \leq x \leq \frac{p-1}{2}\} = \{x^2;\ 1 \leq x \leq \frac{p-1}{2}\}$, módulo p.

Segue então que, módulo p,

$$2^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)^2 P \equiv 1^2 \cdot 2^2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)^2 \left(\prod(x^2+1)\right)^{\frac{p-1}{2}}$$

ou, ainda,

$$2^{\frac{p-1}{2}} P \equiv \left(\prod(x^2+1)\right)^{\frac{p-1}{2}}.$$

Sejam α uma raiz primitiva, módulo p, e $Q = \prod(x^2+1)$. Uma vez que $\{\alpha^{2k};\ 1 \leq k \leq \frac{p-1}{2}\}$ é um conjunto de $\frac{p-1}{2}$ resíduos quadráticos dois a dois incongruentes, módulo p, temos $\{\alpha^{2k};\ 1 \leq k \leq \frac{p-1}{2}\} = \{x^2;\ 1 \leq x \leq \frac{p-1}{2}\}$, módulo p, de sorte que

$$Q = \prod(\alpha^{2k} + 1) \quad \text{e} \quad 2^{\frac{p-1}{2}} P \equiv Q^{\frac{p-1}{2}} \pmod{p}. \tag{7.10}$$

A fim de calcular o resíduo de Q, módulo p, seja $f \in \mathbb{Z}[X]$ definido por

$$f(X) = (X - \alpha^2)(X - \alpha^4) \ldots (X - \alpha^{p-1}),$$

de maneira que

$$Q \equiv (-1)^{\frac{p-1}{2}} f(-1) \equiv -f(-1) \pmod{p}$$

(aqui, utilizamos o fato de que $p \equiv 3 \pmod 4$ na segunda congruência acima).

Agora, observe que

$$f(X^2) = (X-\alpha)(X-\alpha^2)\ldots(X-\alpha^{\frac{p-1}{2}})(X+\alpha)(X+\alpha^2)\ldots(X+\alpha^{\frac{p-1}{2}}).$$

Para $1 \leq i, j \leq \frac{p-1}{2}$, se $\alpha^i \equiv -\alpha^j \pmod{p}$, então $\alpha^{2i} \equiv \alpha^{2j} \pmod{p}$, e segue de α ser uma raiz primitiva, módulo p, que $2i = 2j$ ou, ainda, $i = j$; mas, assim sendo, teríamos $\alpha^i \equiv -\alpha^i \pmod{p}$, o que é um absurdo. Então, o conjunto $\{\pm\alpha, \pm\alpha^2, \ldots, \pm\alpha^{\frac{p-1}{2}}\}$ é um SCI[5], módulo p, de sorte que coincide, módulo p, com $\{1, 2, \ldots, p-1\}$. Portanto, denotando por $\overline{f} \in \mathbb{Z}_p[X]$ a imagem de f pela projeção de $\mathbb{Z}[X]$ sobre $\mathbb{Z}_p[X]$, temos

$$\overline{f}(X^2) = (X - \overline{1})(X - \overline{2})\ldots(X - \overline{p-1}) = X^{p-1} - \overline{1}$$

e, daí,

$$\overline{f}(X) = X^{\frac{p-1}{2}} - \overline{1}.$$

Mas, como $p \equiv 3 \pmod 4$, segue que

$$\overline{Q} = -\overline{f}(-\overline{1}) = -(-\overline{1})^{\frac{p-1}{2}} - \overline{1} = \overline{2},$$

i.e., $Q \equiv 2 \pmod{p}$.

Por fim, substituindo essa informação em (7.10), obtemos a congruência $2^{\frac{p-1}{2}} P \equiv 2^{\frac{p-1}{2}} \pmod{p}$ e, a partir dela, $P \equiv 1 \pmod{p}$. □

Problemas – Seção 7.3

1. * Fixado um primo p, verifique a boa definição das operações de adição e de multiplicação de $\mathbb{Z}_p[X]$. Mostre também que tais operações são associativas e comutativas, possuem elementos neutros respectivamente iguais a $\overline{0}$ e $\overline{1}$ e que a multiplicação é distributiva em relação à adição.

[5]Recorde que um *sistema completo de invertíveis* (abreviamos *SCI*), módulo p, é um conjunto $\{a_1, a_2, \ldots, a_{p-1}$ de inteiros tais que, a menos de uma permutação, temos $a_j \equiv j \pmod{p}$.

2. * Se $f \in \mathbb{Z}[X]$ e $a \in \mathbb{Z}$ é raiz de f, prove que $\overline{a} \in \mathbb{Z}_p$ é raiz de $\overline{f} \in \mathbb{Z}_p[X]$. Em particular, conclua que, se $\overline{a}_1, \ldots, \overline{a}_k \in \mathbb{Z}_p$ são as raízes de $\overline{f}$, então existe $1 \leq j \leq k$ tal que $a \equiv a_j \pmod{p}$.

3. Ache, se houver, as raízes em $\mathbb{Z}_3$ do polinômio $X^2 - \overline{2}X + \overline{1} \in \mathbb{Z}_3[X]$.

4. Fatore $X^2 + \overline{3}$ em $\mathbb{Z}_7[X]$.

5. Mostre que o polinômio $f(X) = X^3 - 15X^2 + 10X - 84$ não tem raízes racionais.

6. * Se $p \in \mathbb{Z}$ é primo e $f \in \mathbb{Z}[X]$, prove que $\overline{f}(X^p) = \overline{f}(X)^p$.

7. * Use a projeção $\pi : \mathbb{Z} \to \mathbb{Z}_p$ para provar que, se $f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$ são polinômios primitivos (conforme a definição 7.11), então fg também o é.

8. * Seja $p \geq 3$ primo e, para $1 \leq j \leq p-1$, seja $s_j(1, 2, \ldots, p-1)$ a j–ésima soma simétrica elementar dos números $1, 2, \ldots, p-1$. Prove que:

   (a) Para $1 \leq j \leq p-2$, temos $s_j(1, 2, \ldots, p-1) \equiv 0 \pmod{p}$.

   (b) $s_{p-1}(1, 2, \ldots, p-1) \equiv -1 \pmod{p}$.

9. * Se a, b e c são as raízes complexas do polinômio $X^3 - 3X^2 + 1$, mostre que, para todo $n \in \mathbb{N}$, a soma $a^n + b^n + c^n$ é inteira e deixa resto 1 quando dividida por 17.

7.4 Irredutibilidade de polinômios

Até o momento, não temos à disposição modo algum de determinar se um dado polinômio é ou não irredutível. É claro que, em exemplos práticos, pode-se, às vezes, utilizar para tal fim o *método direto*, qual

seja, escrever um polinômio dado f (digamos em $\mathbb{Z}[X]$) como produto de dois outros g e h e, resolvendo o sistema de equações resultante nos coeficientes de g e h, obter uma fatoração para f ou chegar a uma contradição. A seguir, exemplificamos tal procedimento (veja, também, os problemas 1 e 2).

Exemplo 7.23. *Prove que $f(X) = X^4 + 10X^3 + 5X + 1993$ é irredutível sobre $\mathbb{Q}$.*

Prova. Pelo lema de Gauss, é suficiente mostrar que f não pode ser escrito como produto de dois polinômios não constantes e de coeficientes inteiros. Para tanto, observe inicialmente que 1993 é primo (pelo critério de Eratóstenes, por exemplo); portanto, pelo critério de pesquisa de raízes inteiras, as possíveis raízes inteiras de f são ± 1 ou ± 1993, e uma verificação direta garante que f não possui raízes inteiras. Resta, pois, descartarmos a possibilidade de fatoração de f na forma

$$f(X) = (X^2 + aX + b)(X^2 + cX + d),$$

com $a, b, c, d \in \mathbb{Z}$. Se tal ocorrer, então, desenvolvendo o produto do segundo membro e igualando os coeficientes obtidos aos correspondentes do primeiro membro, obtemos o sistema de equações

$$\begin{cases} a + c = 10 \\ ac + b + d = 0 \\ ad + bc = 5 \\ bd = 1993 \end{cases}.$$

A quarta equação, juntamente com a primalidade de 1993 e a simetria da fatoração de f, nos fornecem as possibilidades essencialmente distintas $(b, d) = (1, 1993)$ ou $(-1, -1993)$. Portanto, a primeira e a terceira equações fornecem um dos sistemas de equações

$$\begin{cases} a + c = 10 \\ a + 1993c = 5 \end{cases} \quad \text{ou} \quad \begin{cases} a + c = 10 \\ a + 1993c = -5 \end{cases}.$$

Por fim, é imediato verificar que nenhum de tais sistemas possui soluções inteiras. □

Conforme atestam os cálculos executados no exemplo acima, a verificação, pelo método direto, de que um polinômio $f \in \mathbb{Q}[X]$ dado é irredutível sobre $\mathbb{Q}$ esbarra em dificuldades computacionais consideráveis, mesmo no caso em que f tem coeficientes inteiros e grau pequeno. Faz-se, pois, necessário desenvolvermos técnicas apropriadas ao tratamento de questões ligadas à irredutibilidade de polinômios. Nesse sentido, comecemos com o seguinte resultado.

Proposição 7.24. *Sejam $f \in \mathbb{Z}[X]$ primitivo e mônico e $p \in \mathbb{Z}$ primo.*

(a) Se $\overline{f} \in \mathbb{Z}_p[X]$ é irredutível em $\mathbb{Z}_p[X]$, então f é irredutível em $\mathbb{Z}[X]$.

(b) Se $\overline{f}(X) = (X - \overline{a})\overline{f}_1(X)$, com $\overline{f}_1 \in \mathbb{Z}_p[X]$ irredutível, então ou f é irredutível em $\mathbb{Z}[X]$ ou f tem uma raiz $\alpha \in \mathbb{Z}$ tal que $\alpha \equiv a \pmod{p}$.

Prova.
(a) Por contraposição, suponha $f(X) = g(X)h(X)$, com $g, h \in \mathbb{Z}[X] \setminus \mathbb{Z}$ mônicos. Então, $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$, com $\partial\overline{g} = \partial g$ e $\partial\overline{h} = \partial h$.

(b) Suponha f redutível, digamos $f(X) = g(X)h(X)$, com $g, h \in \mathbb{Z}[X] \setminus \mathbb{Z}$ mônicos. Então, $\partial\overline{g} = \partial g$, $\partial\overline{h} = \partial h$ e

$$(X - \overline{a})\overline{f}_1(X) = \overline{g}(X)\overline{h}(X).$$

Mas, uma vez que $\overline{f}_1$ é irredutível em $\mathbb{Z}_p[X]$, segue do teorema 7.20 que $\overline{g}$ ou $\overline{h}$ deve ser associado a $X - \overline{a}$ e, daí, que $\partial g = 1$ ou $\partial h = 1$. Suponha, sem perda de generalidade, que $\partial g = 1$. Então, $\overline{g}(X) = X - \overline{a}$ e g (logo, f) tem uma raiz $\alpha \in \mathbb{Z}$. Por fim, é claro que $\overline{\alpha} = \overline{a}$. □

Exemplo 7.25. *Seja $p \in \mathbb{Z}$ primo e $k \in \mathbb{N}$ tais que $p \equiv 5 \pmod{6}$ e $kp+1$ é primo. Prove que $f(X) = X^3 + pX^2 + pX + kp + 1$ é irredutível em $\mathbb{Z}[X]$.*

Prova. Projetando em $\mathbb{Z}_p[X]$, temos

$$\overline{f}(X) = X^3 + \overline{1} = (X + \overline{1})(X^2 - X + \overline{1}).$$

Afirmamos inicialmente que $-\overline{1}$ é a única raiz de $\overline{f}$ em $\mathbb{Z}_p$. De fato, se $\overline{f}(\overline{a}) = \overline{0}$, então $\overline{a}^3 = -\overline{1}$ e, daí, $a^3 \equiv -1 \pmod{p}$; assim, $a^6 \equiv 1 \pmod{p}$, de maneira que

$$\text{ord}_p(a) \mid \text{mdc}(6, p-1) = 2,$$

i.e., $\text{ord}_p(a) = 1$ ou 2. Mas, como $\text{ord}_p(a) = 1 \Rightarrow \overline{a} = \overline{1}$, o qual não é raiz de $\overline{f}$, devemos ter $\text{ord}_p(a) = 2$. Então, $a^2 \equiv 1 \pmod{p}$ e $a \not\equiv 1 \pmod{p}$, de sorte que $a \equiv -1 \pmod{p}$ ou, ainda, $\overline{a} = -\overline{1}$.

Segue da afirmação acima que $X^2 - X + \overline{1}$ não tem raízes em $\mathbb{Z}_p[X]$ e, portanto, é irredutível em $\mathbb{Z}_p[X]$. A proposição anterior assegura, então, que ou f é irredutível em $\mathbb{Z}[X]$ ou f tem uma raiz $\alpha \in \mathbb{Z}$ tal que $\alpha \equiv -1 \pmod{p}$. Mas, pelo critério de pesquisa de raízes racionais (proposição 3.16), uma raiz α de f deve dividir $kp + 1$, que é primo, de forma que $\alpha = -1$ ou $\alpha = -(kp + 1)$. Testando tais possibilidades, obtemos uma contradição. □

Observação 7.26. *Fixado $p \in \mathbb{N}$, estabeleceremos na seção 8.2 a existência de infinitos $k \in \mathbb{Z}$ tais que $kp + 1$ seja primo.*

O teorema a seguir e, mais precisamente, seu corolário, o **critério de Eisenstein**, se constitui em poderoso aliado na tarefa de garantir a irredutibilidade de certos polinômios.

Teorema 7.27 (Eisenstein). *Seja $f(X) = a_nX^n + \cdots + a_1X + a_0$ um polinômio de grau $n \geq 1$ e com coeficientes inteiros. Sejam ainda $p \in \mathbb{Z}$ primo e $1 \leq k < n$ inteiro tais que:*

(a) $p \mid a_0, a_1, \ldots, a_k$.

(b) $p^2 \nmid a_0$ *e* $p \nmid a_n$.

Se $f = gh$, *com* $g, h \in \mathbb{Z}[X]$, *então ao menos um dentre* g *e* h *tem grau maior ou igual a* $k+1$.

Prova. Se $f(X) = g(X)h(X)$, com $g(X) = b_rX^r + \cdots + b_0$ e $h(X) = c_sX^s + \cdots + c_0$ polinômios em $\mathbb{Z}[X]$, então $a_n = b_rc_s$ e $a_0 = b_0c_0$. Portanto,

$$p \nmid a_n \Rightarrow p \nmid b_rc_s \Rightarrow p \nmid b_r \text{ e } p \nmid c_s,$$

de maneira que, em $\mathbb{Z}_p[X]$, temos $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$, com $\partial\overline{g} = \partial g = r$ e $\partial\overline{h} = \partial h = s$. Ademais, se $X \mid \overline{g}(X)$ e $X \mid \overline{h}(X)$ em $\mathbb{Z}_p[X]$, então $p \mid b_0$ e $p \mid c_0$ em $\mathbb{Z}$, de sorte que $p^2 \mid b_0c_0 = a_0$, o que é um absurdo. Portanto, em $\mathbb{Z}_p[X]$, o polinômio X divide no máximo um dos polinômios $\overline{g}$ ou $\overline{h}$, e segue de

$$\begin{aligned} \overline{g}(X)\overline{h}(X) &= \overline{f}(X) = \overline{a}_nX^n + \cdots + \overline{a}_{k+1}X^{k+1} \\ &= (\overline{a}_nX^{n-k-1} + \cdots + \overline{a}_{k+1})X^{k+1} \end{aligned}$$

que $X^{k+1} \mid \overline{g}(X)$ ou $X^{k+1} \mid \overline{h}(X)$. Logo, $r \geq k+1$ ou $s \geq k+1$. □

Corolário 7.28 (Eisenstein). *Seja* $f(X) = a_nX^n + \cdots + a_1X + a_0$ *um polinômio de grau* $n \geq 1$ *e com coeficientes inteiros. Se existe* $p \in \mathbb{Z}$ *primo tal que* $p \mid a_0, a_1, \ldots, a_{n-1}$, $p^2 \nmid a_0$ *e* $p \nmid a_n$, *então* f *é irredutível em* $\mathbb{Q}[X]$.

Prova. Pelo teorema anterior, se $f(X) = g(X)h(X)$, com $g, h \in \mathbb{Z}[X]$, então $\partial g \geq n$ ou $\partial h \geq n$, de maneira que h ou g é constante. Assim, f não pode ser escrito como o produto de dois polinômios não constantes de coeficientes inteiros, e segue do lema de Gauss que f é irredutível em $\mathbb{Q}[X]$. □

Colecionamos, no exemplo a seguir, uma aplicação clássica do corolário acima, a qual será reobtida, por outros métodos e em maior generalidade, na seção 8.2.

Exemplo 7.29. *Se* $p \in \mathbb{Z}$ *é primo e* $f \in \mathbb{Z}[X]$ *é o polinômio definido por*

$$f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1, \tag{7.11}$$

então f *é irredutível sobre* $\mathbb{Q}$.

Prova. Observando, inicialmente, que $f(X) = g(X)h(X)$ se, e só se, $f(X+1) = g(X+1)h(X+1)$, concluímos ser suficiente provar que $f(X+1)$ é irredutível em $\mathbb{Q}[X]$. Mas, como $(X-1)f(X) = X^p - 1$, temos

$$\begin{aligned} Xf(X+1) &= (X+1)^p - 1 \\ &= X^p + \binom{p}{1}X^{p-1} + \cdots + \binom{p}{p-1}X \end{aligned}$$

e, daí,

$$f(X+1) = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-1}.$$

Agora, lembre-se (conforme exemplo 1.41 de [14]) de que $p \mid \binom{p}{k}$, para $1 \leq k \leq p-1$, de modo que podemos aplicar o critério de Eisenstein com o primo p para concluir pela irredutibilidade de $f(X+1)$ em $\mathbb{Q}[X]$. □

Em que pese a teoria desenvolvida acima, frequentemente estabelecemos a irredutibilidade de um certo polinômio por intermédio de métodos *ad hoc*. Vejamos alguns exemplos.

Exemplo 7.30 (Romênia). *Seja* $f \in \mathbb{Z}[X]$ *um polinômio mônico de grau* $n \geq 1$, *tal que* $f(0) = 1$. *Se* f *tiver pelo menos* $n-1$ *raízes complexas de módulo menor que* 1, *prove que* f *será irredutível em* $\mathbb{Q}[X]$.

Prova. Pelo lema de Gauss, basta mostrar que f é irredutível em $\mathbb{Z}[X]$. Suponha, pois, $f = gh$, com $g, h \in \mathbb{Z}[X] \setminus \mathbb{Z}$. Sem perda de generalidade, podemos supor g e h mônicos. De $g(0)h(0) = 1$, temos

$g(0), h(0) = \pm 1$. Por outro lado, pelas relações de Girard (vide a proposição 4.6), o módulo do produto das raízes complexas de f é igual a 1, de modo que, pelas hipóteses do enunciado, f tem exatamente uma raiz complexa de módulo maior que 1. Portanto, um dos polinômios g ou h, digamos g, tem somente raízes complexas de módulo menor que 1. Mas, uma vez que g é mônico e $|g(0)| = 1$, temos, novamente pelas relações de Girard, que o módulo do produto das raízes de g é igual a 1, o que é uma contradição. □

Observação 7.31. *Polinômios $f \in \mathbb{Z}[X]$ satisfazendo as condições do lema acima podem ser facilmente construídos. Por exemplo, seja $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ tal que*

$$|a_{n-1}| > |a_n| + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|.$$

Se $|z| = 1$, então

$$\begin{aligned} |f(z) - a_{n-1}z^{n-1}| &= |a_nz^n + a_{n-2}z^{n-2} + \cdots + a_1z + a_0| \\ &\le |a_n| + |a_{n-2}| + \cdots + |a_1| + |a_0| \\ &< |a_{n-1}| = |a_{n-1}z^{n-1}|. \end{aligned}$$

Em particular, f não se anula sobre o círculo $|z| = 1$ do plano complexo, e um teorema da teoria de funções analíticas $f : \mathbb{C} \to \mathbb{C}$ (o teorema de Rouché – veja a seção VI.4 de [50], por exemplo) garante que f possui exatamente $n - 1$ raízes complexas de módulo menor que 1.

Exemplo 7.32. *Sejam $n > 1$ um inteiro ímpar e $a_1, \ldots, a_n$ inteiros dados, dois a dois distintos. Prove que o polinômio*

$$f(X) = (X - a_1)(X - a_2) \ldots (X - a_n) - 1$$

é irredutível em $\mathbb{Q}[X]$.

Prova. Pelo lema de Gauss, basta mostrar que f não pode ser escrito como produto de dois polinômios não constantes e de coeficientes inteiros. Suponha, por contradição, que fosse $f = gh$, com g e h polinômios mônicos, de coeficientes inteiros e não constantes. Como

$$g(a_i)h(a_i) = f(a_i) = -1$$

e $g(a_i), h(a_i) \in \mathbb{Z}$, deve ser $g(a_i) = 1$ e $h(a_i) = -1$, ou vice-versa; em qualquer caso, temos $g(a_i) + h(a_i) = 0$. Agora, defina $f_1 = g + h$. Como g e h são mônicos, f_1 não é identicamente nulo. Então,

$$\partial f_1 \le \max\{\partial g, \partial h\} < \partial f = n,$$

de maneira que f_1 admite, no máximo, $\partial f_1 < n$ raízes distintas. Mas, como $f_1(a_i) = 0$ para $1 \le i \le n$, chegamos a uma contradição. □

Problemas – Seção 7.4

1. Use o método direto, descrito no início desta seção, para provar que o polinômo $X^4 - X^2 + 1$ é irredutível em $\mathbb{Z}[X]$.

2. * Também com o auxílio do método direto, mostre que o polinômio $f(X) = X^5 - X^4 - 4X^3 + 4X^2 + 2$ é irredutível sobre $\mathbb{Q}$.

3. Um polinômio de coeficientes reais é dito *positivamente redutível* se puder ser expresso como produto de dois polinômios não constantes, cujos coeficientes não nulos são reais positivos. Seja f um polinômio de coeficientes reais tal que, para algum $n \in \mathbb{N}$, o polinômio $f(X^n)$ é positivamente redutível. Mostre que f é positivamente redutível.

4. Sejam $n > 1$ inteiro e $a_1, \dots, a_n$ inteiros positivos dados, dois a dois distintos. Prove que o polinômio

$$f(X) = (X - a_1)(X - a_2)\dots(X - a_n) + 1$$

é redutível em $\mathbb{Q}[X]$ somente nos seguintes casos:

(a) $f(X) = (X - a)(X - a - 2) + 1$.

(b) $f(X) = (X - a)(X - a - 1)(X - a - 2)(X - a - 3) + 1$.

5. Sejam p um primo ímpar, $f(X) = 2X^{p-1} - 1$ e $g(X) = (X - 1)(X-2)\dots(X-p+1)$. Prove que ao menos um dos polinômios $f(X) - g(X)$ ou $f(X) - g(X) + p$ é irredutível em $\mathbb{Z}[X]$.

6. (IMO.) Prove que o polinômio de coeficientes inteiros $X^n + 5X^{n-1} + 3$ é irredutível em $\mathbb{Z}[X]$.

7. Sejam $p \in \mathbb{Z}$ primo e $f(X) = a_{2n+1}X^{2n+1} + \dots + a_nX^n + \dots + a_1X + a_0$ um polinômio de coeficientes inteiros satisfazendo as seguintes condições:

(a) $p^2 \mid a_0, a_1, \dots, a_n$.

(b) $p \mid a_{n+1}, a_{n+2}, \dots, a_{2n}$.

(c) $p^3 \mid a_0$ e $p \nmid a_{2n+1}$.

Mostre que f não pode ser escrito como o produto de dois polinômios não constantes e de coeficientes inteiros.

8. (Romênia.) Seja $p \in \mathbb{Z}$ um número primo. Se $f(X) = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ é um polinômio de coeficientes inteiros, com $|a_0| = p$ e tal que $|a_n| + |a_{n-1}| + \dots + |a_1| < p$, prove que f é irredutível sobre $\mathbb{Q}$.

9. (Romênia.) Seja $f(X) = a_nX^n + \dots + a_1X + a_0$ um polinômio não constante de coeficientes inteiros. Se $|a_0| > |a_1| + |a_2| + \dots + |a_n|$ e $\sqrt{|a_0|} < \sqrt{|a_n|} + 1$, prove que f não pode ser escrito como o produto de dois polinômios não constantes e de coeficientes inteiros.

10. (Romênia.) Seja $\mathbb{N} = A_1 \cup A_2 \cup \dots \cup A_k$ uma partição do conjunto dos números naturais em k conjuntos não vazios. Dado $m \in \mathbb{N}$, prove que existe $1 \le j \le k$ tal que podemos construir infinitos polinômios f satisfazendo as seguintes condições:

(a) $\partial f = m$.

(b) Os coeficientes de f pertencem ao conjunto A_j.

(c) f não pode ser escrito como o produto de dois polinômios não constantes de coeficientes inteiros.

11. * Sejam f um polinômio de coeficientes inteiros e grau n, e $z_1, \dots, z_n$ as raízes complexas de f.

(a) Se $\mathrm{Re}(z_i) < 0$ para $1 \le i \le n$, prove que todos os coeficientes de f têm um mesmo sinal.

(b) Prove o **teorema de Pólya-Szegö** [6]: suponha que existe $m \in \mathbb{Z}$ tal que $f(m)$ é primo, $f(m-1) \neq 0$ e $m > \frac{1}{2} + \mathrm{Re}(z_i)$, para $1 \le i \le n$. Então, f não pode ser escrito como produto de dois polinômios não constantes e de coeficientes inteiros.

12. (BMO.) Sejam $n > 1$ inteiro e $a_0, a_1, \dots, a_{n-1}, a_n$ naturais tais que $a_n \neq 0$ e $0 \le a_i \le 9$, para $0 \le i \le n$. Se $f(10)$ é primo, prove que f é irredutível sobre $\mathbb{Z}$.

[6] Após os matemáticos húngaros do século XX George Pólya e Gábor Szegö.

CAPÍTULO 8

Números Algébricos e Aplicações

Neste capítulo, invertemos o ponto de vista adotado no capítulo 3. Mais precisamente, fixamos um número complexo z e examinamos o conjunto dos polinômios $f \in \mathbb{C}[X]$ tais que $f(z) = 0$. Como subproduto de nossa discussão, damos uma prova distinta da apresentada em [26] para o fechamento, em relação às operações aritméticas usuais, do conjunto dos números complexos que são raízes de polinômios não nulos e de coeficientes racionais. Por outro lado, a análise do caso em que $z \in \mathbb{C}$ é uma raiz $n-$ésima da unidade nos leva ao estudo dos polinômios ciclotômicos e permite dar uma prova parcial de um famoso teorema de Dirichlet sobre a infinitude de primos em progressões aritméticas.

8.1 Números algébricos

Um número complexo α é dito **algébrico** sobre $\mathbb{Q}$ se existir um polinômio $f \in \mathbb{Q}[X] \setminus \{0\}$ tal que $f(\alpha) = 0$. Um número complexo que não é algébrico sobre $\mathbb{Q}$ é dito **transcendente** sobre $\mathbb{Q}$.

É possível provar (e o faremos na seção 8.3) que nem todo número complexo é algébrico, i.e., que o conjunto dos números transcendentes é não vazio. Por outro lado, é claro que todo racional r, sendo raiz do polinômio $X - r \in \mathbb{Q}[X] \setminus \{0\}$, é algébrico sobre $\mathbb{Q}$. Colecionamos, a seguir, alguns exemplos menos triviais de números algébricos sobre $\mathbb{Q}$.

Exemplo 8.1. *Sejam $r \in \mathbb{Q}_+^*$ e $n \in \mathbb{N}$. Se ω é uma raiz $n-$ésima da unidade, então $\sqrt[n]{r}\omega$ é algébrico sobre $\mathbb{Q}$, uma vez que tal número é raiz do polinômio não nulo de coeficientes racionais $X^n - r$.*

Poderíamos definir, aliás de modo óbvio, o que se entende por um número complexo α ser algébrico sobre $\mathbb{R}$. Contudo, esse não é um conceito interessante, uma vez que todo complexo é algébrico sobre $\mathbb{R}$. De fato, dado um complexo não real $\alpha = a + ib$, temos que α é raiz do polinômio não nulo

$$\begin{aligned} f(X) &= (X - (a + bi))(X - (a - bi)) \\ &= X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]. \end{aligned}$$

Por essa razão, sempre que considerarmos um número algébrico sobre $\mathbb{Q}$, diremos simplesmente que se trata de um número algébrico.

Se um complexo α for algébrico, o conjunto

$$\mathcal{A}_\alpha = \{f \in \mathbb{Q}[X] \setminus \{0\};\ f(\alpha) = 0\}$$

é, por definição, não vazio. Então, também é não vazio o conjunto de inteiros não negativos $\{\partial f;\ f \in \mathcal{A}_\alpha\}$, de modo que existe $p_\alpha \in \mathcal{A}_\alpha$ mônico e de grau mínimo. Temos, pois, a definição a seguir.

Definição 8.2. *Dado α algébrico sobre $\mathbb{Q}$, um polinômio $p_\alpha \in \mathbb{Q}[X] \setminus \{0\}$, mônico, de grau mínimo e tendo α por raiz é denominado um* **polinômio minimal** *de α.*

A proposição a seguir e seus corolários colecionam as propriedades mais importantes de polinômios minimais de números algébricos.

Proposição 8.3. *Se α é algébrico sobre $\mathbb{Q}$ e p_α é um polinômio minimal de α, então:*

(a) p_α é irredutível sobre $\mathbb{Q}$.

(b) Se $f \in \mathbb{Q}[X]$ é tal que $f(\alpha) = 0$, então $p_\alpha \mid f$ em $\mathbb{Q}[X]$.

Em particular, p_α é unicamente determinado por α.

Prova.
(a) Se fosse $p_\alpha = fg$, com f e g não constantes e de coeficientes racionais, então f e g teriam graus menores que o grau de p_α e ao menos um deles teria α por raiz, uma contradição à minimalidade do grau de p_α. Logo, p_α é irredutível sobre $\mathbb{Q}$.

(b) Pelo algoritmo da divisão, existem polinômios $q, r \in \mathbb{Q}[X]$ tais que

$$f(X) = p_\alpha(X)q(X) + r(X),$$

com $r = 0$ ou $0 \leq \partial r < \partial p_\alpha$. Se $r \neq 0$, então

$$r(\alpha) = f(\alpha) - p_\alpha(\alpha)q(\alpha) = 0,$$

com $\partial r < \partial p_\alpha$, novamente contradizendo a minimalidade do grau de p_α. Logo, $r = 0$ e, daí, $p_\alpha \mid f$ em $\mathbb{Q}[X]$.

Por fim, se p_α e q_α são polinômios minimais de α, segue do item (b) que $p_\alpha \mid q_\alpha$ e $q_\alpha \mid p_\alpha$ em $\mathbb{Q}[X]$. Mas, como p_α e q_α são ambos mônicos, temos $p_\alpha = q_\alpha$. □

Graças à proposição anterior, dado $\alpha \in \mathbb{C}$ algébrico, podemos nos referir a p_α como *o* polinômio minimal de α.

Corolário 8.4. *Se $\alpha \in \mathbb{C}$ é algébrico e $f \in \mathbb{Q}[X]\setminus\{0\}$ é um polinômio mônico, irredutível e tal que $f(\alpha) = 0$, então $f = p_\alpha$.*

Prova. Pela proposição anterior, p_α divide f em $\mathbb{Q}[X]$. Mas, como f é irredutível, deve existir um racional não nulo c tal que $f = cp_\alpha$. Por fim, como f e p_α são mônicos, devemos ter $c = 1$. □

Corolário 8.5. *Se $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ é irredutível, então f não possui raízes múltiplas.*

Prova. Podemos supor, sem perda de generalidade, que f é mônico. Se algum $\alpha \in \mathbb{C}$ fosse raiz múltipla de f, então a proposição 3.31 garantiria que α também seria raiz da derivada f' de f. Mas, como $f \in \mathbb{Q}[X] \setminus \{0\}$ é mônico e irredutível, o corolário 8.4 garantiria que f é o polinômio minimal de α. Portanto, teríamos, pela proposição 8.3, que $f \mid f'$ em $\mathbb{Q}[X]$, contradizendo a desigualdade $\partial f > \partial f'$. □

Colecionamos, agora, alguns exemplos de aplicação da proposição 8.3 e de seus corolários.

Exemplo 8.6. *Sejam f um polinômio não constante de coeficientes racionais e α um número real tal que $\alpha^3 - 3\alpha = f(\alpha)^3 - 3f(\alpha) = -1$. Prove que, para todo inteiro positivo n, tem-se*

$$f^{(n)}(\alpha)^3 - 3f^{(n)}(\alpha) = -1,$$

onde $f^{(n)}$ denota a composição de f consigo mesmo, n vezes.

Prova. Se $g(X) = X^3 - 3X + 1$, então $\partial g = 3$ e, pelo critério de pesquisa de raízes racionais (a proposição 3.16), g não tem raízes racionais. Portanto, pelo problema 3, página 163, g é irredutível sobre $\mathbb{Q}$. Daí, o corolário 8.4 garante que g é o polinômio minimal de α.

Por outro lado, como estamos supondo que o polinômio $g \circ f$ também tem α por raiz, a proposição 8.3 garante que g divide $g \circ f$ em $\mathbb{Q}[X]$, digamos $(g \circ f)(X) = g(X)u(X)$, para algum $u(X) \in \mathbb{Q}[X]$.

Por fim, suponha que tenhamos provado que $g(f^{(k)}(\alpha)) = 0$ para algum $k \geq 1$. Então

$$g(f^{k+1}(\alpha)) = (g \circ f)(f^k(\alpha)) = g(f^k(\alpha))u(f^k(\alpha)) = 0,$$

e nada mais há a fazer. □

O exemplo 7.29, em conjunção com o corolário 8.4, garante imediatamente que, se p é primo e $\omega = \text{cis}\,\frac{2\pi}{p}$, então o polinômio minimal de ω é

$$p_\omega(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

O próximo exemplo utiliza este fato para dar uma bela prova alternativa do exemplo 6.4 de [14], devida ao matemático búlgaro N. Nikolov.

Exemplo 8.7 (IMO). *Seja p um primo ímpar. Calcule quantos subconjuntos de p elementos do conjunto $\{1, 2, \ldots, 2p\}$ são tais que a soma de seus elementos é divisível por p.*

Solução. Se $\omega = \text{cis}\,\frac{2\pi}{p}$, então $\omega^p = 1$ e segue, daí, que

$$\begin{aligned}(X^p - 1)^2 &= \prod_{j=1}^{p}(X - \omega^j)\prod_{j=1}^{p}(X - \omega^j)\\ &= \prod_{j=1}^{p}(X - \omega^j)\prod_{j=p+1}^{2p}(X - \omega^j)\\ &= \prod_{j=1}^{2p}(X - \omega^j).\end{aligned}$$

Calculando o coeficiente de X^p em ambos os membros da igualdade acima e lembrando que p é ímpar, concluímos que

$$2 = \sum_{\{j_1,\ldots,j_p\}\subset I_{2p}} \omega^{j_1+\cdots+j_p}, \tag{8.1}$$

onde a soma acima se estende a todos os subconjuntos de p elementos, $\{j_1, \ldots, j_p\}$, de $I_{2p} = \{1, 2, \ldots, 2p\}$.

Por outro lado, se, para $0 \leq k \leq p-1$, denotarmos por c_k o número de conjuntos de p elementos $\{j_1, \ldots, j_p\} \subset I_{2p}$, tais que $j_1 + \cdots + j_p \equiv k \pmod p$, então $\omega^p = 1$ garante que o segundo membro de (8.1) é igual a $\sum_{k=0}^{p-1} c_k \omega^k$, de sorte que

$$\sum_{k=0}^{p-1} c_k \omega^k = 2.$$

Segue do que fizemos acima que ω é raiz do polinômio de coeficientes inteiros $f(X) = \sum_{k=0}^{p-1} c_k X^k - 2$. Note ainda que $c_{p-1} \neq 0$, uma vez que o conjunto

$$\left\{1, p-1, 2, p-2, 3, p-3, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, 2p-1\right\}$$

tem p elementos e a soma dos mesmos é congruente a $p-1$, módulo p. Portanto, $\partial f = p - 1$.

Mas, como o polinômio minimal de ω é $p_\omega(X) = X^{p-1} + \cdots + X + 1$, o item (b) da proposição 8.3 garante que f é um múltiplo inteiro de p_ω, digamos $f = cp_\omega$, com $c \in \mathbb{N}$. Em particular, comparando os coeficientes de ambos os membros dessa igualdade, concluímos que

$$c_0 - 2 = c_1 = \cdots = c_{p-1} = c.$$

A fim de calcular o valor de c, note que $c_0 + c_1 + \cdots + c_{p-1}$ é igual ao número de subconjuntos de p elementos de I_{2p}, de maneira que

$$pc + 2 = c_0 + c_1 + \cdots + c_{p-1} = \binom{2p}{p}.$$

Logo,

$$c_0 = c + 2 = \frac{1}{p}\left(\binom{2p}{p} - 2\right) + 2.$$

□

Exemplo 8.8 (Romênia). *Seja $f \in \mathbb{Z}[X]$ um polinômio mônico, de grau ímpar maior que 1 e irredutível sobre $\mathbb{Q}$. Suponha ainda que:*

(a) $f(0)$ é livre de quadrados.

(b) As raízes complexas de f têm módulo maior ou igual a 1.

Prove que o polinômio $F \in \mathbb{Z}[X]$, dado por $F(X) = f(X^3)$, também é irredutível sobre $\mathbb{Q}$.

Prova. Por contradição, suponha que F é redutível sobre $\mathbb{Q}$. Então, segue do problema 2, página 168, a existência de polinômios $g, h \in \mathbb{Z}[X]$, mônicos, não constantes e tais que $F = gh$. Como $\partial F = 3\partial f$ e ∂f é ímpar, segue que ∂F também é ímpar. Portanto, o problema 4, página 75, garante que F admite uma raiz real α.

Podemos supor, sem perda de generalidade, que α é raiz de g e que g é irredutível sobre $\mathbb{Q}$. De fato, se α for raiz de g mas g for redutível sobre $\mathbb{Q}$, basta tomar o fator mônico e irredutível de g que tem α por raiz, utilizando em seguida o resultado do problema 2, página 168, para concluir que tal fator irredutível tem coeficientes inteiros.

Nas condições do parágrafo anterior, sabemos que g é o polinômio minimal de α sobre $\mathbb{Q}$. Agora, se ω é uma raiz cúbica de 1, com $\omega \neq 1$, então

$$0 = F(\alpha) = f(\alpha^3) = f((\alpha\omega)^3) = F(\alpha\omega) = g(\alpha\omega)h(\alpha\omega).$$

Temos, pois, de distinguir dois casos:

(i) $g(\alpha\omega) = 0$: como (pelo problema 2, página 74) as raízes não reais de um polinômio de coeficientes reais ocorrem aos pares complexo-complexo conjugado, temos que $\overline{\alpha\omega} = \alpha\omega^2$ também é raiz de g. Agora, agrupando na expressão de g os monômios com expoentes das formas $3k$, $3k+1$ e $3k+2$, podemos escrever

$$g(X) = a(X^3) + Xb(X^3) + X^2c(X^3), \tag{8.2}$$

com a, b e c de coeficientes inteiros. Logo,

$$a(\alpha^3) + \alpha b(\alpha^3) + \alpha^2 c(\alpha^3) = g(\alpha) = 0,$$

$$a(\alpha^3) + \alpha\omega b(\alpha^3) + \alpha^2\omega^2 c(\alpha^3) = g(\alpha\omega) = 0,$$

e

$$a(\alpha^3) + \alpha\omega^2 b(\alpha^3) + \alpha^2\omega c(\alpha^3) = g(\alpha\omega^2) = 0.$$

Considerando as três igualdades acima como um sistema linear de equações em $a(\alpha^3)$, $b(\alpha^3)$ e $c(\alpha^3)$, não é difícil mostrar que $a(\alpha^3) = b(\alpha^3) = c(\alpha^3) = 0$. Assim, sendo p o polinômio minimal de α^3 sobre $\mathbb{Q}$, segue da proposição 8.3 que p divide a, b e c em $\mathbb{Q}[X]$ e, portanto (novamente pelo problema 2, página 74), em $\mathbb{Z}[X]$. Segue de (8.2) que $p(X^3)$ divide $g(X)$. Mas, como g é mônico e irredutível, concluímos que $g(X) = p(X^3)$. Agora, sendo g um polinômio em X^3, segue novamente de (8.2) que $b, c = 0$ e, daí, que

$$f(X^3) = F(X) = g(X)h(X) = a(X^3)h(X).$$

Tal igualdade, por sua vez, implica que h também deve ser um polinômio em X^3, digamos $h(X) = l(X^3)$, com $l \in \mathbb{Z}[X]$. Finalmente, temos $f(X^3) = a(X^3)l(X^3)$ e, daí, $f = gl$, com $\partial g, \partial l \geq 1$. Mas isto contraria a irredutibilidade de f.

(ii) $h(\alpha\omega) = 0$: como no item (i), concluímos que $h(\alpha\omega^2) = 0$. Seja, ainda como acima,

$$h(X) = a(X^3) + Xb(X^3) + X^2c(X^3),$$

com a, b e c de coeficientes inteiros. Então,

$$a(\alpha^3) + \alpha\omega b(\alpha^3) + \alpha^2\omega^2 c(\alpha^3) = h(\alpha\omega) = 0$$

e

$$a(\alpha^3) + \alpha\omega^2 b(\alpha^3) + \alpha^2\omega c(\alpha^3) = h(\alpha\omega^2) = 0.$$

Multiplicando a primeira dessas igualdades por ω e subtraindo a segunda do resultado, obtemos

$$a(\alpha^3) - \alpha^2 c(\alpha^3) = 0.$$

Mas, como g é o polinômio minimal de α sobre $\mathbb{Q}$, invocando novamente a proposição 8.3, concluímos que g divide $a(X^3) - X^2c(X^3)$ em $\mathbb{Q}[X]$ e, logo, em $\mathbb{Z}[X]$ (pela observação 2.11, uma vez que $g \in \mathbb{Z}[X]$ e é mônico). Fazendo $X = 0$, concluímos que $g(0)$ deve dividir $a(0)$ em $\mathbb{Z}$. Sendo $a(0) = g(0)m$, com $m \in \mathbb{Z}$, segue que

$$f(0) = g(0)h(0) = g(0)a(0) = g(0)^2m.$$

Uma vez que $f(0)$ é livre de quadrados, segue que $g(0) = \pm 1$. Portanto, sendo $z_1, \ldots, z_k$ as raízes complexas de g, segue das relações de Girard que

$$1 = |g(0)| = |z_1| \ldots |z_k|. \tag{8.3}$$

Por outro lado, como

$$f(z_j^3) = F(z_j) = g(z_j)h(z_j) = 0,$$

segue do item (b) do enunciado que $|z_j^3| \geq 1$ e, portanto, $|z_j| \geq 1$, para $1 \leq j \leq k$. Coligindo tal informação com (8.3), concluímos que $|z_j| = 1$, para $1 \leq j \leq k$. Em particular, $|\alpha| = 1$ e, sendo α real, devemos ter $\alpha = \pm 1$, de sorte que $\alpha^3 = \pm 1$. Mas, como f é irredutível sobre $\mathbb{Q}$ e $f(\alpha^3) = 0$, teríamos $f(X) = X \pm 1$, contrariando o fato de que $\partial f > 1$. □

O restante desta seção é destinado a apresentar uma demonstração de que o conjunto dos números complexos algébricos é fechado para as operações de adição, subtração, multiplicação e divisão (por um divisor algébrico não nulo). Começamos com o seguinte resultado.

Teorema 8.9. *Se $\alpha, \beta \in \mathbb{C} \setminus \{0\}$ são algébricos, então $\alpha + \beta$ também o é.*

Prova. Sejam $\alpha = \alpha_1, \ldots, \alpha_m$ as raízes complexas de p_α e $\beta = \beta_1, \ldots, \beta_n$ aquelas de p_β, de modo que

$$p_\alpha(X) = \prod_{i=1}^{m}(X - \alpha_i) \text{ e } p_\beta(X) = \prod_{j=1}^{n}(X - \beta_j).$$

Defina

$$\begin{aligned} f(X, X_1, \ldots, X_m) &= \prod_{i=1}^{m}\prod_{j=1}^{n}(X - X_i - \beta_j) = \prod_{i=1}^{m} p_\beta(X - X_i) \\ &= X^{mn} + \sum_{k=0}^{mn-1} f_k(X_1, \ldots, X_m)X^k, \end{aligned}$$

para certos polinômios $f_0, \ldots, f_{mn-1} \in \mathbb{Q}[X_1, \ldots, X_m]$ (uma vez que $p_\beta \in \mathbb{Q}[X]$).

Se σ é uma permutação de I_m, então

$$\begin{aligned} f(X, X_{\sigma(1)}, \ldots, X_{\sigma(m)}) &= \prod_{i=1}^{m} p_\beta(X - X_{\sigma(i)}) = \prod_{i=1}^{m} p_\beta(X - X_i) \\ &= f(X, X_1, \ldots, X_m) \end{aligned}$$

ou, ainda,

$$X^{mn} + \sum_{k=0}^{mn-1} f_k(X_{\sigma(1)}, \ldots, X_{\sigma(m)})X^k = X^{mn} + \sum_{k=0}^{mn-1} f_k(X_1, \ldots, X_m)X^k.$$

Portanto, temos

$$f_k(X_{\sigma(1)}, \ldots, X_{\sigma(m)}) = f_k(X_1, \ldots, X_m),$$

para todos $0 \leq k \leq mn - 1$ e σ, de sorte que f_k é um polinômio simétrico em $X_1, \ldots, X_m$, para $0 \leq k \leq mn - 1$.

O teorema de Newton 4.12 garante, então, a existência de um polinômio $g_k \in \mathbb{Q}[X_1, \ldots, X_m]$ tal que

$$f_k(X_1, \ldots, X_m) = g_k(s_1, \ldots, s_m),$$

onde $s_1, \ldots, s_m \in \mathbb{Q}[X_1, \ldots, X_m]$ são os polinômios simétricos elementares em $X_1, \ldots, X_m$. Em particular,

$$f_k(\alpha_1, \ldots, \alpha_m) = g_k(s_1(\alpha_i), \ldots, s_m(\alpha_i)) \in \mathbb{Q},$$

uma vez que

$$p_\alpha(X) = X^m - s_1(\alpha_i)X^{m-1} + \cdots + (-1)^m s_m(\alpha_i) \in \mathbb{Q}[X].$$

Assim, se $h(X) = f(X, \alpha_1, \ldots, \alpha_m)$, então, por um lado,

$$h(X) = X^{mn} + \sum_{k=0}^{mn-1} f_k(\alpha_1, \ldots, \alpha_m)X^k \in \mathbb{Q}[X]$$

e, por outro,

$$h(X) = \prod_{i=1}^{m} p_\beta(X - \alpha_i) = \prod_{i=1}^{m}\prod_{j=1}^{n}(X - \alpha_i - \beta_j).$$

Logo, h é um polinômio não nulo de coeficientes racionais, tal que $h(\alpha + \beta) = 0$, o que garante que $\alpha + \beta$ é algébrico. □

Observação 8.10. *Suponha que $p_\alpha, p_\beta \in \mathbb{Z}[X]$. Então, nas notações da demonstração acima, temos $s_1(\alpha_i), \ldots, s_m(\alpha_i) \in \mathbb{Z}$, e $f_k \in \mathbb{Z}[X_1, \ldots, X_m]$, para $0 \leq k \leq mn - 1$. Portanto, segue novamente do teorema de Newton que $g_k \in \mathbb{Z}[X_1, \ldots, X_m]$ e, daí, que*

$$f_k(\alpha_1, \ldots, \alpha_m) = g_k(s_1(\alpha_i), \ldots, s_m(\alpha_i)) \in \mathbb{Z},$$

para $0 \leq k \leq mn - 1$. Portanto, $h \in \mathbb{Z}[X]$ e segue do problema 4 que $p_{\alpha+\beta} \in \mathbb{Z}[X]$.

Para mostrar que o conjunto dos números algébricos é fechado para produtos e quocientes, precisamos do seguinte resultado auxiliar.

Lema 8.11. *Se $\alpha \neq 0$ é algébrico, então α^{-1} e α^2 também o são.*

Prova. Seja $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tal que $a_0 \neq 0$ e $f(\alpha) = 0$. Então, $g(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$ é um polinômio não constante de coeficientes racionais, e é imediato verificar que $g(\alpha^{-1}) = 0$.

Para α^2, observe que existem polinômios u e v de coeficientes racionais, não ambos nulos e tais que

$$f(X) = u(X^2) + Xv(X^2).$$

Sendo $h(X) = u(X)^2 - Xv(X)^2$, temos $h \in \mathbb{Q}[X] \setminus \{0\}$ e

$$\begin{aligned} h(\alpha^2) &= u(\alpha^2)^2 - \alpha^2 v(\alpha^2)^2 \\ &= (u(\alpha^2) - \alpha v(\alpha^2))(u(\alpha^2) + \alpha v(\alpha^2)) \\ &= (u(\alpha^2) - \alpha v(\alpha^2))f(\alpha) = 0. \end{aligned}$$

□

Teorema 8.12. *Se $\alpha, \beta \in \mathbb{C}\setminus\{0\}$ são algébricos, então $\alpha\beta$ e $\frac{\alpha}{\beta}$ também o são.*

Prova. Pelo lema anterior, α^2 e β^2 são algébricos. Mas, como já sabemos que $\alpha + \beta$ é algébrico, segue novamente do lema anterior que $(\alpha + \beta)^2$ também o é. Agora, uma vez que

$$\alpha\beta = \frac{1}{2}((\alpha + \beta)^2 - \alpha^2 - \beta^2),$$

duas aplicações do teorema 8.9, juntamente com o resultado do problema 1, garantem que $\alpha\beta$ é algébrico.

Para o que falta, observe que $\frac{\alpha}{\beta} = \alpha \cdot \frac{1}{\beta}$, com $\frac{1}{\beta}$ algébrico (pelo lema anterior). Portanto, a primeira parte acima garante que $\frac{\alpha}{\beta}$ é algébrico. □

Problemas – Seção 8.1

1. * Se r é um racional não nulo e $\alpha \neq 0$ é um complexo algébrico, prove diretamente (i.e., sem recorrer ao teorema 8.12) que $r\alpha$ também é algébrico.

2. Dado $n \in \mathbb{N}$, prove que $\cos \frac{2\pi}{n}$ é um número algébrico.

3. Sejam p primo e $n \in \mathbb{N}$. Prove que o polinômio minimal de $\sqrt[n]{p}$ é $f(X) = X^n - p$.

4. * Seja $\alpha \in \mathbb{C}$ algébrico. Se existe $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ mônico e tal que $f(\alpha) = 0$, prove que $p_\alpha \in \mathbb{Z}[X]$.

5. (a) Sejam a, b e c inteiros positivos. Prove que:
   (i) $\sqrt{a} + \sqrt{b} + \sqrt{c}$ é raiz de um polinômio mônico e de coeficientes inteiros.
   (ii) Se $\sqrt{a}+\sqrt{b}+\sqrt{c} \notin \mathbb{Z}$, então $\sqrt{a}+\sqrt{b}+\sqrt{c}$ é irracional.
   (b) Generalize os itens (i) e (ii) para $\sqrt{b_1} + \sqrt{b_2} + \cdots + \sqrt{b_n}$, onde $b_1, b_2, \ldots, b_n$ são inteiros positivos.

6. (OBM.) Prove que o polinômio $f(X) = X^5 - X^4 - 4X^3 + 4X^2 + 2$ não admite raízes da forma $\sqrt[n]{r}$, onde r é um racional e $n > 1$ é um natural.

7. Dê uma prova análoga à do teorema 8.9 para mostrar que $\alpha\beta$ é algébrico sempre que α e β o são.

8.2 Polinômios ciclotômicos

A teoria de polinômios sobre $\mathbb{Z}_p$, p primo, nos permite apresentar algumas das propriedades elementares de uma classe muito importante de polinômios, conhecidos como *ciclotômicos*. Como subproduto do

estudo que faremos aqui, mostraremos que os polinômios ciclotômicos são exatamente os polinômios minimais das raízes complexas da unidade.

Sendo n um natural e $\omega_n = \text{cis}\,\frac{2\pi}{n}$, consideraremos, no que segue, as raízes n–ésimas da unidade da forma ω_n^k, com $1 \leq k \leq n$ e $\text{mdc}\,(k,n) = 1$. Tais raízes são ditas **primitivas**, e é imediato que há exatamente $\varphi(n)$ de tais raízes, onde $\varphi : \mathbb{N} \to \mathbb{N}$ é a função de Euler. Dados $m, n \in \mathbb{N}$, sempre que não houver perigo de confusão denotaremos seu mdc escrevendo simplesmente (m,n).

Definição 8.13. *Para $n \in \mathbb{N}$, o* **n–ésimo polinômio ciclotômico** *é o polinômio*

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (X - \omega_n^k). \tag{8.4}$$

Segue da definição acima que Φ_n é mônico e $\partial\Phi_n = \varphi(n)$. A proposição a seguir coleciona outras propriedades elementares de Φ_n.

Proposição 8.14. *Para $n \in \mathbb{N}$, temos:*

(a) $X^n - 1 = \prod_{0<d|n} \Phi_d(X)$.

(b) $\Phi_n \in \mathbb{Z}[X]$.

(c) $\Phi_n(0) = 1$, *para* $n > 1$.

Prova.
(a) Observe inicialmente que

$$\prod_{0<d|n} \Phi_d(X) = \prod_{0<d|n} \Phi_{n/d}(X) = \prod_{0<d|n} \prod_{\substack{1 \leq k \leq n/d \\ (k,n/d)=1}} (X - \omega_{n/d}^k)$$
$$= \prod_{0<d|n} \prod_{\substack{1 \leq k \leq n/d \\ (k,n/d)=1}} (X - \omega_n^{dk}).$$

Agora, como cada inteiro $1 \leq m \leq n$ pode ser escrito de modo único como $m = dk$, com $0 < d \mid n$ e $\left(k, \frac{n}{d}\right) = 1$ (tal d é $d = (m,n)$), a última soma acima é claramente igual a

$$\prod_{j=1}^{n} (X - \omega_n^j) = X^n - 1.$$

(b) Façamos indução sobre $n \in \mathbb{N}$, notando inicialmente que $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$, por definição. Seja, agora, $n > 1$ natural e suponha, por hipótese de indução, que $\Phi_m \in \mathbb{Z}[X]$, para todo inteiro $1 \leq m < n$. Se

$$g(X) = \prod_{\substack{1 \leq d < n \\ d|n}} \Phi_d(X),$$

temos que $g \in \mathbb{Z}[X]$ e, pelo item (a), $X^n - 1 = \Phi_n(X) g(X)$. Mas, como g é mônico (pois já sabemos que cada Φ_m o é), segue da observação 2.11 que $\Phi_n \in \mathbb{Z}[X]$.

(c) Novamente por indução, temos primeiramente

$$X^2 - 1 = \Phi_1(X)\Phi_2(X) = (X-1)\Phi_2(X),$$

de modo que $\Phi_2(X) = X + 1$ e $\Phi_2(0) = 1$. Seja, agora, $n > 1$ e suponha, por hipótese de indução, que $\Phi_m(0) = 1$ para todo inteiro $2 \leq m < n$. Então, nas notações da prova de (b), temos

$$g(0) = \Phi_1(0) \prod_{\substack{1<d<n \\ d|n}} \Phi_d(0) = (-1) \prod_{\substack{1<d<n \\ d|n}} \Phi_d(0) = -1,$$

e segue de $X^n - 1 = \Phi_n(X) g(X)$ que

$$-1 = \Phi_n(0) g(0) = -\Phi_n(0),$$

como desejado. □

Corolário 8.15. *Se p é primo, então*

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Prova. O item (a) da proposição anterior garante que

$$X^p - 1 = \Phi_1(X)\Phi_p(X) = (X-1)\Phi_p(X),$$

de sorte que

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

□

O exemplo 7.29 mostrou que Φ_p é irredutível sobre $\mathbb{Q}$, de sorte que Φ_p é o polinômio minimal de ω_p. No que segue, nosso objetivo é generalizar este fato, provando que, para todo $n \in \mathbb{N}$, o polinômio minimal p_{ω_n} de ω_n coincide com o $n-$ésimo polinômio ciclotômico Φ_n. Precisamos, inicialmente, do seguinte resultado auxiliar.

Lema 8.16. *Sejam $f, g \in \mathbb{Z}[X]$ e $p \in \mathbb{N}$ um número primo. Se $\overline{g} \in \mathbb{Z}_p[X] \setminus \mathbb{Z}_p$ e $\overline{g}^2 \mid \overline{f}$ em $\mathbb{Z}_p[X]$, então $\overline{g} \mid \overline{f'}$ em $\mathbb{Z}_p[X]$.*

Prova. Se $h \in \mathbb{Z}[X]$ é tal que $\overline{f}(X) = \overline{g}(X)^2\overline{h}(X)$ em $\mathbb{Z}_p[X]$, sabemos que existe um polinômio $l \in \mathbb{Z}[X]$ tal que

$$f(X) = g(X)^2h(X) + pl(X)$$

em $\mathbb{Z}[X]$. Derivando ambos os membros dessa igualdade, obtemos

$$f'(X) = 2g(X)g'(X)h(X) + g(X)^2h'(X) + pl'(X)$$

em $\mathbb{Z}[X]$ e, daí,

$$\overline{f'}(X) = \overline{g}(X)(\overline{2}\,\overline{g'}(X)\overline{h}(X) + \overline{g}(X)\overline{h'}(X))$$

em $\mathbb{Z}_p[X]$. Logo, $\overline{g} \mid \overline{f'}$ em $\mathbb{Z}_p[X]$. □

Para o próximo resultado, lembre-se de que, se ω é uma raiz $n-$ésima da unidade, então a proposição 8.3 garante que seu polinômio minimal p_ω divide $X^n - 1$ em $\mathbb{Q}[X]$. Em particular, segue do problema 4, página 201, que $p_\omega \in \mathbb{Z}[X]$.

Proposição 8.17. *Sejam $n, p \in \mathbb{N}$ tais que p é primo e $p \nmid n$. Se ω é uma raiz $n-$ésima da unidade, então $p_\omega(X) = p_{\omega^p}(X)$.*

Prova. Seja $\zeta = \omega^p$. Como ω e ζ são ambos raízes de $X^n - 1$, o item (b) da proposição 8.3 garante que $p_\omega(X)$ e $p_\zeta(X)$ dividem $X^n - 1$. Por contradição, suponha que $p_\omega(X) \neq p_\zeta(X)$. Então, a irredutibilidade de tais polinômios garante, via teorema 7.15, que $p_\omega(X)p_\zeta(X)$ divide $X^n - 1$ em $\mathbb{Z}[X]$, digamos

$$X^n - 1 = p_\omega(X)p_\zeta(X)u(X). \tag{8.5}$$

Se $g(X) = p_\zeta(X^p)$, então

$$g(w) = p_\zeta(\omega^p) = p_\zeta(\zeta) = 0$$

e, daí, p_ω divide g em $\mathbb{Z}[X]$. Seja $v \in \mathbb{Z}[X]$ tal que $p_\omega(X)v(X) = g(X)$. Em $\mathbb{Z}_p[X]$, temos pelo problema 6, página 178, que

$$\overline{p}_\omega(X)\overline{v}(X) = \overline{g}(X) = \overline{p}_\zeta(X^p) = \left(\overline{p}_\zeta(X)\right)^p,$$

e o teorema 7.20 garante a existência de um polinômio mônico e irredutível $\overline{h} \in \mathbb{Z}_p[X]$ tal que $\overline{h}(X) \mid \overline{p}_\omega(X), \overline{p}_\zeta(X)$ em $\mathbb{Z}_p[X]$. Segue de (8.5) que $\overline{h}(X)^2 \mid (X^n - \overline{1})$ em $\mathbb{Z}_p[X]$, e o lema anterior garante que $\overline{h}(X) \mid \overline{n}X^{n-1}$ em $\mathbb{Z}_p[X]$. Mas, como $\overline{h}$ é mônico e $\overline{n} \neq \overline{0}$, aplicando novamente o teorema 7.20 obtemos $1 \leq l \leq n-1$ tal que $\overline{h}(X) = X^l$ em $\mathbb{Z}_p[X]$. Logo, $\overline{h}(X) \nmid (X^n - \overline{1})$ em $\mathbb{Z}_p[X]$, o que é uma contradição. □

Chegamos finalmente ao resultado desejado.

Teorema 8.18. *Se $\omega_n = \text{cis}\,\frac{2\pi}{n}$, então $p_{\omega_n} = \Phi_n$. Em particular, $\Phi_n \in \mathbb{Z}[X]$ é irredutível sobre $\mathbb{Q}[X]$.*

Prova. Tome $k \in \mathbb{N}$ tal que $k > 1$ e $\operatorname{mdc}(k,n) = 1$, e seja $k = p_1 \dots p_l$, com $p_1, \dots, p_l$ primos que não dividem n. Repetidas aplicações da proposição anterior nos dão

$$p_{\omega_n} = p_{\omega_n^{p_1}} = p_{\omega_n^{p_1 p_2}} = \dots = p_{\omega_n^{p_1 \cdots p_l}} = p_{\omega_n^k}.$$

Em particular, os $\varphi(n)$ números ω_n^k, com $1 \leq k \leq n$ e $\operatorname{mdc}(k,n) = 1$, são raízes distintas de p_{ω_n}, de maneira que

$$\partial p_{\omega_n} \geq \varphi(n) = \partial \Phi_n.$$

Mas, como Φ_n é mônico de coeficientes inteiros e tem ω_n por raiz, a definição de polinômio minimal garante que $p_{\omega_n} = \Phi_n$. □

Terminamos esta seção provando um caso particular do teorema de Dirichlet sobre primos em progressões aritméticas. Esse teorema afirma que uma progressão aritmética não constante e infinita de números naturais contém uma infinidade de números primos, contanto que sua razão e seu primeiro termo sejam relativamente primos. Em que pese o teorema de Dirichlet ser uma generalização natural do teorema de Euclides da infinitude dos primos (este último provado na seção 1.3 de [14]), as provas conhecidas desse resultado estão fora do alcance da maior parte dos currículos de graduação em Matemática. Todavia, a teoria de polinômios ciclotômicos desenvolvida acima nos permite apresentar uma demonstração elementar do teorema de Dirichlet, no caso particular em que o primeiro termo da progressão é igual a 1.

Teorema 8.19 (Dirichlet). *Se $n \in \mathbb{N}$, então a PA $1, 1+n, 1+2n, \dots$ contém infinitos números primos.*

Prova. Sejam $p_1, \dots, p_k$ primos quaisquer e Φ_n o $n-$ésimo polinômio ciclotômico. Como Φ_n é mônico, escolhendo um inteiro y suficientemente grande, temos $\Phi_n(ynp_1 \dots p_k) > 1$. Agora, fazendo

$a = ynp_1 \dots p_k$ temos, módulo a, que

$$\Phi_n(a) \equiv \Phi_n(0) = 1 \pmod{a}.$$

Seja, então, $\Phi_n(a) = aq + 1 = ynp_1 \dots p_k q + 1$. Se p for um fator primo de $\Phi_n(a)$, temos $p \neq p_1, \dots, p_k$ e $\operatorname{mdc}(p,n) = 1$. Portanto, se provarmos que $p \equiv 1 \pmod{n}$, seguirá que p é um primo em nossa PA, diferente de $p_1, \dots, p_k$.

Para o que falta, note que $\operatorname{mdc}(p,a) = 1$, de modo que podemos considerar $t := \operatorname{ord}_p(a)$. Como $p \mid \Phi_n(a)$ e $\Phi_n(a) \mid (a^n - 1)$ (pois $\Phi_n(X) \mid (X^n - 1)$ em $\mathbb{Z}[X]$), vem que $a^n \equiv 1 \pmod{p}$ e, daí, $t \mid n$. Se mostrarmos que $t = n$, seguirá das propriedades da ordem e de $a^{p-1} \equiv 1 \pmod{p}$ que $n \mid (p-1)$ ou, o que é o mesmo, $p \equiv 1 \pmod{n}$.

Se $c \in \{a, a+p\}$, segue de $a^t \equiv 1 \pmod{p}$ que $c^t \equiv 1 \pmod{p}$. Suponha, por contradição, que $t < n$. A proposição 8.14, juntamente com o fato de que $t \mid n$, nos dá

$$\begin{aligned} c^n - 1 &= \prod_{0<d|n} \Phi_d(c) = \Phi_n(c) \prod_{\substack{0<d<n \\ d|n}} \Phi_d(c) \\ &= \Phi_n(c)h(c) \prod_{0<d|t} \Phi_d(c) \\ &= \Phi_n(c)h(c)(c^t - 1), \end{aligned}$$

onde $h \in \mathbb{Z}[X]$ é um polinômio apropriado. Mas, como $c \equiv a \pmod{p}$, segue que

$$\Phi_n(c) \equiv \Phi_n(a) \equiv 0 \pmod{p},$$

de maneira que

$$c^n - 1 = \Phi_n(c)h(c)(c^t - 1) \equiv 0 \pmod{p^2}.$$

Por outro lado,

$$(a+p)^n - 1 = a^n - 1 + \sum_{j=1}^{n-1} \binom{n}{j} a^{n-j} p^j$$

e (pelos cálculos acima) tanto $(a+p)^n-1$ quanto a^n-1 são múltiplos de p^2. Portanto, olhando a última igualdade acima módulo p^2, concluímos que

$$na^{n-1}p \equiv 0 \pmod{p^2},$$

o que é um absurdo. □

Para uma discussão autocontida da prova do caso geral, sugerimos ao leitor as referências [37] ou [51].

Problemas – Seção 8.2

1. Sendo p primo e k natural, calcule explicitamente o polinômio Φ_{p^k}.

2. Se $n > 1$ é um inteiro par, mostre que $\Phi_{2n}(X) = \Phi_{2n}(-X)$.

3. Se m e n são naturais distintos, prove que Φ_m e Φ_n não têm fatores não constantes comuns em $\mathbb{C}[X]$.

4. Se $n > 1$ é natural e d é o produto dos fatores primos distintos de n, mostre que
$$\Phi_n(X) = \Phi_d\left(X^{n/d}\right).$$

5. O conjunto $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$ contém várias progressões aritméticas. Prove que, dado $k > 2$ inteiro, esse conjunto contém uma progressão de k termos que não está contida em uma progressão de $k+1$ termos do conjunto.

6. Sejam $a, n \in \mathbb{N}$, sendo $a > 1$ e n ímpar. Prove que a congruência $x^n \equiv a \pmod{p}$ tem solução para uma infinidade de primos p.

7. Seja $a \in \mathbb{N}$ não quadrado perfeito. Prove que há infinitos primos p tais que a não é resíduo quadrático, módulo p.

8. Sejam $a, b \in \mathbb{Z}$ tais que, para cada $n \in \mathbb{N}$, existe um inteiro c para o qual $n \mid (c^2+ac+b)$. Prove que a equação $x^2+ax+b=0$ tem raízes inteiras.

8.3 Números transcendentes

Como foi dito no início da seção 8.1, números transcendentes são precisamente os números complexos que não são raízes de polinômio não nulo algum com coeficientes racionais. Contudo, até esse ponto nem mesmo sabemos se tais números existem.

Uma maneira possível de estabelecer a existência de números transcendentes (mesmo reais) é começar mostrando que o conjunto $\mathcal{A}$ dos números algébricos (reais) é *enumerável*, i.e., que seus elementos podem ser listados como os termos de uma sequência $(x_n)_{n\geq 1}$, de modo que $\mathcal{A} = \{x_1, x_2, x_3, \ldots\}$; então, mostra-se que o conjunto $\mathbb{R}$ não é enumerável, de forma que $\mathbb{R} \setminus \mathcal{A}$ é necessariamente não vazio. Não seguiremos esse caminho aqui, uma vez que ele requeriria que desenvolvêssemos os resultados básicos sobre conjuntos enumeráveis, bem como que estabelecêssemos a não enumerabilidade do conjunto dos reais, e isso nos desviaria bastante do fio condutor deste volume. Para o leitor interessado, sugerimos [26] ou [39].

Em vez de seguir a estratégia delineada no parágrafo anterior, apresentamos a construção (explícita) do primeiro número transcendente descoberto, devida ao matemático francês do século XIX J. Liouville. Nossa apresentação segue o maravilhoso clássico [19].

Para o que segue, dizemos que um número algébrico α tem **grau** n se seu polinômio minimal p_α tem grau n; em particular, se $n > 1$, então é claro que α é irracional. Precisamos introduzir mais uma nomenclatura: dizemos que uma propriedade $P(k)$, dependente de um natural k, é *verdadeira para todo k suficientemente grande* se existe $k_0 \in \mathbb{N}$ tal que $P(k)$ é verdadeira sempre que $k > k_0$; ademais, se

um valor específico de k_0 for irrelevante no contexto sob discussão, escreveremos simplesmente que $P(k)$ é verdadeira para todo $k \gg 1$.

Estamos finalmente em posição de enunciar e provar o teorema de Liouville.

Teorema 8.20 (Liouville). *Seja $\alpha \in \mathbb{C}$ um número algébrico de grau $n > 1$. Se $(p_k)_{k\geq 1}$ e $(q_k)_{k\geq 1}$ são sequências de inteiros não nulos tais que $\lim_{k\to+\infty} \frac{p_k}{q_k} = \alpha$, então*

$$\left|\alpha - \frac{p_k}{q_k}\right| > \frac{1}{q_k^{n+1}}, \tag{8.6}$$

para todo $k \gg 1$.

Prova. Seja $\alpha_k = \frac{p_k}{q_k}$. Como $\alpha_k \xrightarrow{k} \alpha$, temos que $q_k \xrightarrow{k} +\infty$. Como α é algébrico de grau $n > 1$, existe $f \in \mathbb{Z}[X] \setminus \{0\}$ de grau n e tal que $f(\alpha) = 0$, digamos,

$$f(X) = a_n X^n + \cdots + a_1 X + a_0,$$

com $a_0, a_1, \ldots, a_n \in \mathbb{Z}$.

Agora, observemos que

$$\begin{aligned}\left|\frac{f(\alpha_k)}{\alpha_k - \alpha}\right| &= \frac{1}{|\alpha_k - \alpha|} \cdot |f(\alpha_k) - f(\alpha)| \\ &= \frac{1}{|\alpha_k - \alpha|} \cdot \left|\sum_{j=1}^{n} a_j(\alpha_k^j - \alpha^j)\right| \\ &\leq \frac{1}{|\alpha_k - \alpha|} \cdot \sum_{j=1}^{n} |a_j| \cdot |\alpha_k^j - \alpha^j|,\end{aligned}$$

onde utilizamos a desigualdade triangular na última passagem acima. Portanto, um pouco de álgebra elementar fornece

$$\begin{aligned}\left|\frac{f(\alpha_k)}{\alpha_k - \alpha}\right| &\leq \sum_{j=1}^{n} |a_j| \cdot \frac{|\alpha_k^j - \alpha^j|}{|\alpha_k - \alpha|} \\ &= \sum_{j=1}^{n} |a_j| \cdot \left|\alpha_k^{j-1} + \alpha_k^{j-2}\alpha + \cdots + \alpha^{j-1}\right|.\end{aligned} \tag{8.7}$$

Como $\alpha_k \xrightarrow{k} \alpha$, temos $|\alpha_k - \alpha| < 1$ para todo $k \gg 1$. Utilizando a desigualdade triangular, concluímos que

$$|\alpha_k| \leq |\alpha_k - \alpha| + |\alpha| < 1 + |\alpha| \tag{8.8}$$

para todo $k \gg 1$ e, daí, (8.7) e (8.8) fornecem

$$\begin{aligned}\left|\frac{f(\alpha_k)}{\alpha_k - \alpha}\right| &= \sum_{j=1}^{n} |a_j| \Big(|\alpha_k|^{j-1} + |\alpha_k|^{j-2}|\alpha| + \cdots + |\alpha|^{j-1}\Big) \\ &\leq \sum_{j=1}^{n} |a_j| \Big(\big(1 + |\alpha|\big)^{j-1} + \big(1 + |\alpha|\big)^{j-2}|\alpha| + \cdots + |\alpha|^{j-1}\Big) \\ &< \sum_{j=1}^{n} j|a_j|\big((1 + |\alpha|\big)^{j-1},\end{aligned}$$

para todo $k \gg 1$, onde

$$C := \sum_{j=1}^{n} j|a_j|\big((1 + |\alpha|\big)^{j-1}$$

depende somente de α, e não de k.

Então, para todo $k \gg 1$ (escolhido de forma tal que $|\alpha_k - \alpha| < 1$), temos

$$\left|\alpha - \frac{p_k}{q_k}\right| = |\alpha_k - \alpha| > \frac{1}{C}|f(\alpha_k)|.$$

Agora, uma vez que $q_k \xrightarrow{k} +\infty$, temos $|\alpha_k - \alpha| < 1$ e $q_k > C$ para todo $k \gg 1$, de forma que $\frac{1}{C} > \frac{1}{q_k}$ e, portanto,

$$\left|\alpha - \frac{p_k}{q_k}\right| > \frac{1}{q_k}|f(\alpha_k)|,$$

para todo $k \gg 1$.

Como passo final, observe que se $f(\alpha_k) = 0$, então teríamos $f(X) = (X - \alpha_k)g(X)$ para algum $g \in \mathbb{Z}[X] \setminus \{0\}$ de grau $n - 1$. Como $\alpha \neq \alpha_k$

(pois α é irracional), concluímos que α seria raiz de g, contradizendo o fato do polinômio minimial de α ter grau n. Logo, $f(\alpha_k) \neq 0$ e, assim

$$\begin{aligned} |f(\alpha_k)| &= a_n\left(\frac{p_k}{q_k}\right)^n + \cdots + a_1\left(\frac{p_k}{q_k}\right) + a_0 \\ &= \frac{1}{q_k^n}\left|a_n p_k^n + \cdots + a_1 p_k q_k^{n-1} + a_0 q_k^n\right| \\ &\geq \frac{1}{q_k^n}. \end{aligned}$$

Finalmente, combinando essa última desigualdade com a anterior a ela, obtemos (8.6). □

O exemplo a seguir, também devido a Liouville, traz uma aplicação engenhosa do teorema anterior à construção de números transcendentes. Para uma apreciação adequada do mesmo, o leitor precisa possuir uma relativa familiaridade com manipulações aritméticas de séries convergentes, no nível do capítulo 3 de [12].

Exemplo 8.21 (Liouville). *Se $a_1, a_2, a_3, \ldots \in \{1, 2, 3, \ldots, 9\}$, então o número real*

$$\alpha = \frac{a_1}{10^{1!}} + \frac{a_2}{10^{2!}} + \frac{a_3}{10^{3!}} + \cdots.$$

é trancendente.

Prova. Suponha que α fosse algébrico, de grau $n > 1$ (α é claramente irracional – veja o problema 1). Para $k \geq 1$, seja

$$\alpha_k = \sum_{j=1}^{k} \frac{a_j}{10^{j!}} = \frac{p_k}{10^{k!}},$$

com $p_k \in \mathbb{N}$. Então, por um lado, segue do teorema de Liouville que

$$|\alpha - \alpha_k| > \frac{1}{\left(10^{k!}\right)^{n+1}},$$

para todo $k \gg 1$. Por outro,

$$|\alpha - \alpha_k| = \left|\sum_{j>k} \frac{a_j}{10^{j!}}\right| < \frac{1}{10^{(k+1)!}} \cdot 9,999\ldots = \frac{1}{10^{(k+1)!-1}}.$$

Portanto, para $k \gg 1$ teríamos

$$\frac{1}{10^{(k+1)!-1}} > \frac{1}{\left(10^{k!}\right)^{n+1}}$$

e, daí, $(k+1)! - 1 < k!(n+1)$. Contudo, essa última desigualdade equivale a

$$k!(k-n) < 1,$$

que é falsa para $k \geq n+1$.

Finalmente, uma vez que a hipótese de que α é algébrico leva a uma contradição, não temos alternativa além de concluir que α é transcendente. □

Terminamos recordando que, em [12], mostramos que os números e e π são irracionais. Contudo, métodos mais refinados de Análise real permitem mostrar que tais números são transcendentes. Ambos tais fatos foram estabelecidos ainda no século XIX, sendo devidos ao matemático francês C. Hermite e ao matemático alemão F. Lindemann, respectivamente. Para o leitor interessado, recomendamos [26].

Exemplo 8.22. *Admitindo a transcendência dos números e e π, os teoremas 8.9 e 8.12 permitem justificar a transcendência de vários números complexos. Por exemplo, o número $\pi + \sqrt{2}$ é transcendente, posto que, se fosse algébrico, teríamos*

$$\pi = (\pi + \sqrt{2}) - \sqrt{2},$$

também algébrico, por ser uma diferença entre dois números algébricos.

Problemas – Seção 8.3

1. Prove que o número α do Exemplo 8.21 é irracional (esse fato foi utilizado na discussão do exemplo).

2. Assumindo a transcendência de e e de π, prove diretamente (i.e., sem apelar para o teorema 8.9) que os números $\pi+\sqrt{2}$ e $e+\sqrt{3}$ também são transcendentes.

3. Se $\alpha \in \mathbb{C}$ é transcendente e $n \in \mathbb{N}$, prove que $\sqrt[n]{\alpha}$ e α^n também são transcendentes.

CAPÍTULO 9

Recorrências Lineares

Neste capítulo final, completamos o trabalho iniciado na seção 4.3 de [10], mostrando como resolver uma recorrência linear de coeficientes constantes e ordem qualquer. Precisamos, inicialmente, de duas definições, as quais se revelarão centrais para tudo o que segue.

Definição 9.1. *Uma sequência* $(a_n)_{n\geq 1}$ *é dita* **recorrente linear**, *se existirem um inteiro positivo* k *e números complexos* $u_0, \ldots, u_{k-1}$, *nem todos nulos, tais que*

$$a_{n+k} = u_{k-1}a_{n+k-1} + \cdots + u_0 a_n, \tag{9.1}$$

para todo $n \geq 1$.

O natural k é denominado a **ordem** da recorrência linear e a equação (9.1) é a **relação de recorrência** ou, simplesmente, a **recorrência** satisfeita pela sequência. Neste caso, $(a_n)_{n\geq 1}$ é também denominada uma *recorrência linear de ordem* k.

Dados $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$, é imediato verificar que há exatamente uma sequência $(a_n)_{n\geq 1}$ satisfazendo (9.1) e tal que $a_j = \alpha_j$, para $1 \leq j \leq k$. Portanto, uma recorrência linear de ordem k fica totalmente determinada quando conhecemos a relação de recorrência linear por ela satisfeita e os valores de seus k primeiros termos.

Definição 9.2. *Seja $(a_n)_{n\geq 1}$ uma sequência satisfazendo a recorrência linear*

$$a_{n+k} = u_{k-1}a_{n+k-1} + \cdots + u_0 a_n,$$

para $n \geq 1$, onde $u_0, \ldots, u_{k-1}$ são números complexos dados, nem todos nulos. O **polinômio característico** *de $(a_n)_{n\geq 1}$ é o polinômio $f \in \mathbb{C}[X]$ dado por*

$$f(X) = X^k - u_{k-1}X^{k-1} - \cdots - u_1 X - u_0. \tag{9.2}$$

9.1 Um caso particular importante

Discutimos, inicialmente, o caso em que as raízes do polinômio característico da recorrência são duas a duas distintas; apesar da limitação envolvida, este caso é bem mais simples que o caso geral e encontra muitas aplicações interessantes. O resultado de interesse é o conteúdo do teorema a seguir.

Teorema 9.3. *Seja $(a_n)_{n\geq 1}$ uma sequência satisfazendo, para todo $n \geq 1$, a relação de recorrência*

$$a_{n+k} = u_{k-1}a_{n+k-1} + \cdots + u_0 a_n,$$

onde $u_0, \ldots, u_{k-1}$ são números complexos dados, nem todos nulos. Se as raízes complexas z_1, z_2, ..., z_k do polinômio característico de $(a_n)_{n\geq 1}$ são todas distintas e $a_j = \alpha_j$ para $1 \leq j \leq k$, então

$$a_n = z_1^{n-1}x_1 + z_2^{n-1}x_2 + \cdots + z_k^{n-1}x_k, \ \forall n \geq 1,$$

onde $x_1, \ldots, x_k$ é a solução do sistema de Vandermonde

$$\begin{cases} x_1 + x_2 + \cdots + x_k & = \alpha_1 \\ z_1x_1 + z_2x_2 + \cdots + z_kx_k & = \alpha_2 \\ z_1^2x_1 + z_2^2x_2 + \cdots + z_k^2x_k & = \alpha_3 \\ \cdots & \\ z_1^{n-1}x_1 + z_2^{n-1}x_2 + \cdots + z_k^{k-1}x_k & = \alpha_k \end{cases}. \tag{9.3}$$

Prova. Como $z_1, z_2, \ldots, z_k$ são dois a dois distintos, a proposição 6.6 garante a existência de uma única solução $x_1, x_2, \ldots, x_k$ do sistema (9.3). Podemos, pois, definir a sequência $(b_n)_{n\geq 1}$ pondo

$$b_n = z_1^{n-1}x_1 + z_2^{n-1}x_2 + \cdots + z_k^{n-1}x_k, \ \forall n \geq 1.$$

Então, para $1 \leq j \leq k$, o sistema (9.3) fornece

$$b_j = z_1^{j-1}x_1 + z_2^{n-1}x_2 + \cdots + z_k^{j-1}x_k = \alpha_j = a_j.$$

Por outro lado, sendo f o polinômio característico de $(a_n)_{n\geq 1}$, segue da definição dos b_j's que

$$\begin{aligned} & b_{n+k} - u_{k-1}b_{n+k-1} - \cdots - u_0 b_n = \\ = & \sum_{j=1}^{k} z_j^{n+k-1}x_j - u_{k-1}\sum_{j=1}^{k} z_j^{n+k-2}x_j - \cdots - u_0\sum_{j=1}^{k} z_j^{n-1}x_j \\ = & \sum_{j=1}^{k} z_j^{n-1}x_j(z_j^k - u_{k-1}z_j^{k-1} - \cdots - u_0) \\ = & \sum_{j=1}^{k} z_j^{n-1}x_j f(z_j) = 0. \end{aligned}$$

Portanto, a sequência $(b_n)_{n\geq 1}$ satisfaz a mesma recorrência linear que $(a_n)_{n\geq 1}$ e seus k primeiros termos coincidem, respectivamente, com os k primeiros termos da sequência $(a_n)_{n\geq 1}$. Logo, uma fácil indução garante que $a_n = b_n$ para todo $n \geq 1$, conforme desejado. $\square$

O exemplo a seguir mostra que não necessariamente precisamos conhecer explicitamente as raízes do polinômio característico para aplicar o resultado do teorema anterior a fim de obter informações relevantes acerca do comportamento de uma dada recorrência linear.

Exemplo 9.4 (Crux). *Seja $A_1A_2A_3A_4$ o quadrado de vértices $A_1 = (0,1)$, $A_2 = (1,1)$, $A_3 = (1,0)$ e $A_4 = (0,0)$. Para cada $n \geq 1$, seja A_{n+4} o ponto médio do segmento A_nA_{n+1}. Prove que, quando $n \to +\infty$, a sequência de pontos A_n converge para um ponto A e calcule as coordenadas de tal ponto.*

Prova. Para cada $n \geq 1$, seja $A_n(x_n, y_n)$. A condição do enunciado, juntamente com a fórmula para as coordenadas do ponto médio de um segmento (veja o corolário 6.2 de [11]), garante que

$$2x_{n+4} = x_{n+1} + x_n, \ \forall\, n \geq 1,$$

valendo uma recorrência análoga para a sequência $(y_n)_{n\geq 1}$.

O polinômio característico da recorrência acima é

$$f(X) = 2X^4 - X - 1 = (X-1)g(X),$$

onde $g(X) = 2X^3 + 2X^2 + 2X + 1$. Se a, b e c são as raízes complexas de g, segue das relações de Girard que

$$a + b + c = -1 \ \text{ e } \ ab + ac + bc = 1. \tag{9.4}$$

Portanto,

$$a^2 + b^2 + c^2 = (a+b+c)^2 - 2(ab+ac+bc) = (-1)^2 - 2\cdot 1 = -1 < 0,$$

de sorte que, pelo exemplo 4.7 e problema 2, página 74, podemos supor que a é real e b e c são complexos não reais, conjugados. Em particular, a, b e c são dois a dois distintos e, como 1 não é raiz de g,

o teorema 9.3 garante a existência de constantes reais A, B, C e D tais que

$$x_n = Aa^{n-1} + Bb^{n-1} + Cc^{n-1} + D, \ \forall\, n \geq 1. \tag{9.5}$$

Para sabermos o que ocorre quando $n \to +\infty$, note inicialmente que $g(-1)g(0) = -1 < 0$ e, assim, o teorema de Bolzano 5.2 garante que $-1 < a < 0$. Portanto, as relações (9.4) fornecem

$$1 = a(b+c) + bc = a(-1-a) + b\bar{b},$$

de modo que $|b|^2 = a(a+1) + 1 < 1$. Mas, como $|b| = |c|$, segue que $|b| = |c| < 1$. Então, a relação (9.5), juntamente com o resultado do exemplo 9.8, garante que

$$\lim_{n\to+\infty} x_n = D.$$

A fim de calcular o valor de D, recorde que $x_1 = x_4 = 0$ e $x_2 = x_3 = 1$. Portanto, fazendo sucessivamente $n = 1$, 2, 3 e 4 em (9.5), obtemos o sistema linear

$$\begin{cases} A + B + C + D & = 1 \\ Aa + Bb + Cc + Dd & = 0 \\ Aa^2 + Bb^2 + Cc^2 + Dd^2 & = 0 \\ Aa^3 + Bb^3 + Cc^3 + Dd^3 & = 1 \end{cases}.$$

Multiplicando as três últimas equações por 2 e somando membro a membro as quatro igualdades resultantes, chegamos a

$$Ag(a) + Bg(b) + Cg(c) + 7D = 3.$$

Mas, uma vez que a, b e c são as raízes de g, segue que $7D = 3$ ou, ainda, $D = \frac{3}{7}$.

De modo análogo, provamos que $\lim_{n\to+\infty} y_n = \frac{4}{7}$ e, assim,

$$\lim_{n\to+\infty} A_n = \left(\frac{3}{7}, \frac{4}{7}\right).$$

□

Problemas – Seção 9.1

1. Seja $A_1A_2A_3$ o triângulo do plano cartesiano de vértices $A_1(0,0)$, $A_2(1,0)$ e $A_3\left(\frac{1}{2},0\right)$. Para cada $n \geq 1$, seja A_{n+3} o baricentro do triângulo $A_nA_{n+1}A_{n+2}$. Se $A_n(x_n, y_n)$, mostre que $x_n \to \frac{7}{12}$ e $y_n \to \frac{\sqrt{3}}{4}$ quando $n \to +\infty$.

2. Se a é a maior raiz positiva do polinômio $X^3 - 3X^2 + 1$, mostre que os números $\lfloor a^{1788} \rfloor$ e $\lfloor a^{1988} \rfloor$ são, ambos, múltiplos de 17.

9.2 Sequências, séries e continuidade em $\mathbb{C}$

Nesta seção, estendemos algumas definições e resultados dos capítulos 3 e 4 de [12] a funções com valores complexos. Observamos que o material aqui apresentado (mais precisamente, o teorema 9.19) foi utilizado na prova do teorema fundamental da álgebra, na seção 3.3, e será de fundamental importância para a discussão do material da seção 9.3.

Dados $a \in \mathbb{C}$ e $R > 0$, denotamos por $D(a;R)$ o **disco aberto** de centro a e raio R, i.e., o subconjunto de $\mathbb{C}$ dado por

$$D(a;R) = \{z \in \mathbb{C};\ |z-a| < R\}.$$

Analogamente, o **disco fechado** de centro a e raio R é o subconjunto $\overline{D(a;R)}$ de $\mathbb{C}$, dado por

$$\overline{D(a;R)} = \{z \in \mathbb{C};\ |z-a| \leq R\}.$$

Um conjunto $U \subset \mathbb{C}$ é **aberto** se, para todo $a \in U$, existir $R > 0$ tal que $D(a;R) \subset U$. Um conjunto $F \subset \mathbb{C}$ é **fechado** se $F^c = \mathbb{C}\backslash F$ for aberto. É imediato que $\emptyset$ e $\mathbb{C}$ são subconjuntos abertos de $\mathbb{C}$ (no caso de $\emptyset$, não há como a condição exigida pela definição não ser satisfeita, uma vez que não existe $z \in \emptyset$); portanto, $\mathbb{C} = \mathbb{C}\backslash\emptyset$ e $\emptyset = \mathbb{C}\backslash\mathbb{C}$ também são fechados. Colecionamos, a seguir, um exemplo menos trivial.

Exemplo 9.5. *Para todos $a \in \mathbb{C}$ e $R > 0$ o disco aberto $D(a;R)$ é um conjunto aberto e o disco fechado $\overline{D(a;R)}$ é um conjunto fechado.*

Prova. Escolhido arbitrariamente $z \in D(a;R)$, seja $r = R - |z-a|$. Então, $r > 0$ e afirmamos que $D(z;r) \subset D(a;R)$ (veja a figura 9.1), o que será suficiente para garantir que $D(a;R)$ é aberto.

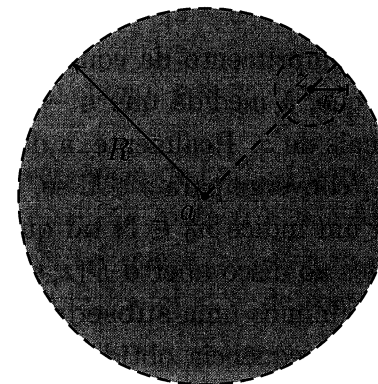



Figura 9.1: todo disco aberto é um conjunto aberto.

Para o que falta, tome $w \in D(z;r)$. Pela desigualdade triangular, temos

$$\begin{aligned} |w-a| &= |(w-z)+(z-a)| \leq |w-z| + |z-a| \\ &\leq r + |z-a| = R \end{aligned}$$

e, daí, $w \in D(a;R)$. Mas, como tal sucede com todo $w \in D(z;r)$, concluímos que $D(z;r) \subset D(a;R)$, conforme desejado.

Para a segunda parte, é suficiente mostrar que $U = \mathbb{C} \setminus \overline{D(a;R)}$ é aberto. Para tanto, tome $z \in U$ e seja $r = |z-a| - R$. Então, $r > 0$ e, como no primeiro caso, mostramos facilmente que $w \in D(z;r) \Rightarrow w \in U$, de sorte $D(z;r) \subset U$. Logo, U é, realmente, aberto. $\square$

Voltemo-nos, agora, às sequências de números complexos, estendendo, às mesmas, o conceito de *convergência*.

Definição 9.6. *Dizemos que uma sequência* $(z_n)_{n\geq 1}$ *em* $\mathbb{C}$ **converge** *para um* **limite** $z \in \mathbb{C}$, *e denotamos* $z_n \to z$ *ou* $\lim_{n\to+\infty} z_n = z$, *se a seguinte condição for satisfeita:*

$$\forall \epsilon > 0,\ \exists n_0 \in \mathbb{N};\ n > n_0 \Rightarrow |z_n - z| < \epsilon.$$

Heuristicamente, o cumprimento da condição estipulada pela definição acima significa que, à medida que $n \to +\infty$, os termos z_n se aproximam cada vez mais de z. Realmente, a definição dada estipula que a sequência $(z_n)_{n\geq 1}$ converge para $z \in \mathbb{C}$ se, dado arbitrariamente um raio $\epsilon > 0$, existir um índice $n_0 \in \mathbb{N}$ tal que os termos z_n, para $n > n_0$, pertençam todos ao disco aberto $D(z;\epsilon)$.

Para o que segue, definimos uma **subsequência** $(z_{n_k})_{k\geq 1}$ de uma sequência $(z_n)_{n\geq 1}$ como a sequência obtida pela restrição de $(z_n)_{n\geq 1}$ a um subconjunto infinito $\{n_1 < n_2 < n_3 < \cdots\}$ de índices; de um ponto de vista mais rigoroso, $(z_{n_k})_{k\geq 1}$ é a sequência $f \circ g : \mathbb{N} \to \mathbb{C}$, onde $f : \mathbb{N} \to \mathbb{C}$ e $g : \mathbb{N} \to \mathbb{N}$ são dadas por $f(n) = z_n$, para todo $n \in \mathbb{N}$, e $g(k) = n_k$, para todo $k \in \mathbb{N}$.

O resultado a seguir encerra duas propriedades fundamentais do conceito de convergência de sequências de números complexos. O item (a) do mesmo garante que os termos de uma sequência convergente não podem se aproximar de dois limites distintos.

Lema 9.7. *Seja* $(z_n)_{n\geq 1}$ *uma sequência em* $\mathbb{C}$.

(a) Se $z_n \to z$ *e* $z_n \to w$, *então* $z = w$.

(b) Se $(z_{n_k})_{k\geq 1}$ *é uma subsequência de* $(z_n)_{n\geq 1}$ *e* $z_n \to z$, *então* $z_{n_k} \to z$.

Prova.
(a) Se $z \neq w$, então $\epsilon = |z - w| > 0$. Mas, como $\frac{\epsilon}{2}$ ainda é positivo e $z_n \to z$ e $z_n \to w$, existem naturais n_1 e n_2 tais que $|z_n - z| < \frac{\epsilon}{2}$ para $n > n_1$ e $|z_n - w| < \frac{\epsilon}{2}$ para $n > n_2$. Portanto, tomando um índice $n > n_1, n_2$ e aplicando a desigualdade triangular, obtemos

$$\begin{aligned} |z - w| &= |(z - z_n) + (z_n - w)| \leq |z - z_n| + |z_n - w| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon = |z - w|, \end{aligned}$$

o que é uma contradição. Logo, $z = w$.

(b) Dado $\epsilon > 0$, a convergência de $(z_n)_{n\geq 1}$ para z garante a existência de $n_0 \in \mathbb{N}$ tal que $|z_n - z| < \epsilon$, para $n > n_0$. Agora, como $n_1 < n_2 < n_3 < \cdots$, existe $k_0 \in \mathbb{N}$ tal que $k > k_0 \Rightarrow n_k > n_0$. Portanto, para tais valores de k, temos $|z_{n_k} - z| < \epsilon$, de sorte que $(z_{n_k})_{k\geq 1}$ também converge para z. □

Graças ao item (a) do lema anterior, se uma sequência $(z_n)_{n\geq 1}$ em $\mathbb{C}$ converge para $z \in \mathbb{C}$, diremos, doravante, que z é *o* limite de $(z_n)_{n\geq 1}$.

Para os propósitos destas notas, um dos exemplos mais importantes de sequência convergente é o isolado a seguir. A esse respeito, veja também o problema 2.

Exemplo 9.8. *Se* $|z| < 1$ *e* $z_n = z^n$, *para todo* $n \geq 1$, *então* $(z_n)_{n\geq 1}$ *converge para* 0.

Prova. Inicialmente, observe que $|z_n - 0| = |z^n| = |z|^n$. Agora, se $(a_n)_{n\geq 1}$ é a sequência de números reais dada por $a_n = |z|^n$, para $n \geq 1$, então o exemplo 3.3 de [12] garante que $a_n \to 0$. Portanto, dado $\epsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $0 \leq a_n < \epsilon$, para $n > n_0$. Assim, para $n > n_0$, temos $|z_n - 0| = a_n < \epsilon$, de sorte que $z_n \to 0$. □

Dada uma sequência $(z_n)_{n\geq 1}$ de números complexos, podemos escrever $z_n = x_n + iy_n$, para todo $n \geq 1$, com $x_n, y_n \in \mathbb{R}$. O próximo

resultado relaciona a convergência da sequência $(z_n)_{n\geq 1}$ em $\mathbb{C}$ com as convergências das sequências $(x_n)_{n\geq 1}$ e $(y_n)_{n\geq 1}$ em $\mathbb{R}$.

Lema 9.9. *Seja $(z_n)_{n\geq 1}$ uma sequência de números complexos, com $z_n = x_n + iy_n$, para todo $n \geq 1$, onde $x_n, y_n \in \mathbb{R}$. Então, $(z_n)_{n\geq 1}$ converge em $\mathbb{C}$ se, e só se, $(x_n)_{n\geq 1}$ e $(y_n)_{n\geq 1}$ convergem em $\mathbb{R}$. Ademais, se $x_n \to a$ e $y_n \to b$, para certos $a, b \in \mathbb{R}$, então $z_n \to z$, onde $z = a + ib$.*

Prova. Suponha, primeiramente, que $z_n \to z$, onde $z = a + ib$, com $a, b \in \mathbb{R}$, e seja dado $\epsilon > 0$. Como

$$|x_n - a|, |y_n - b| \leq \sqrt{|x_n - a|^2 + |y_n - b|^2} = |z_n - z|,$$

temos $|x_n - a|, |y_n - b| < \epsilon$ se $|z_n - z| < \epsilon$. Mas, como $z_n \to z$, existe $n_0 \in \mathbb{N}$ tal que $n > n_0 \Rightarrow |z_n - z| < \epsilon$. Então, para cada um de tais n, temos realmente que $|x_n - a|, |y_n - b| < \epsilon$, o que estabelece as convergências desejadas.

Reciprocamente, suponha que $x_n \to a$ e $y_n \to b$, e seja dado $\epsilon > 0$. Como

$$|z_n - z| = \sqrt{|x_n - a|^2 + |y_n - b|^2} \leq |x_n - a| + |y_n - b|,$$

teremos $|z_n - z| < \epsilon$ se $|x_n - a|, |y_n - b| < \frac{\epsilon}{2}$. Mas, como $x_n \to a$ e $y_n \to b$, existem $n_1, n_2 \in \mathbb{N}$ tais que $n > n_1 \Rightarrow |x_n - a| < \frac{\epsilon}{2}$ e $n > n_2 \Rightarrow |y_n - b| < \frac{\epsilon}{2}$. Se $n_0 = \max\{n_1, n_2\}$, então, para $n > n_0$, temos $|x_n - a|, |y_n - b| < \frac{\epsilon}{2}$ e, daí, $|z_n - z| < \epsilon$, o que estabelece a convergência desejada. □

Precisamos, agora, da definição a seguir.

Definição 9.10. *Uma sequência $(z_n)_{n\geq 1}$ em $\mathbb{C}$ é* **de Cauchy** *se, dado $\epsilon > 0$, existir $n_0 \in \mathbb{N}$ tal que*

$$m, n > n_0 \Rightarrow |z_m - z_n| < \epsilon.$$

Se $(z_n)_{n\geq 1}$ é uma sequência convergente em $\mathbb{C}$, então $(z_n)_{n\geq 1}$ é de Cauchy. De fato, se $z_n \to z$ e $\epsilon > 0$ é dado, então existe $n_0 \in \mathbb{N}$ tal que $|z_n - z| < \frac{\epsilon}{2}$, para todo $n > n_0$. Portanto, para $m, n > n_0$, segue da desigualdade triangular para números complexos que

$$|z_m - z_n| \leq |z_m - z| + |z - z_n| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Reciprocamente, temos o seguinte resultado.

Proposição 9.11. $\mathbb{C}$ *é* **completo**. *Mais precisamente, se $(z_n)_{n\geq 1}$ é uma sequência de Cauchy em $\mathbb{C}$, então $(z_n)_{n\geq 1}$ converge.*

Prova. Seja $z_n = x_n + iy_n$, com $(x_n)_{n\geq 1}$ e $(y_n)_{n\geq 1}$ sequências de números reais. Dado $\epsilon > 0$, tome $n_0 \in \mathbb{N}$ como na definição de sequência de Cauchy. Como $|x_m - x_n| \leq |z_m - z_n|$, segue que $(x_n)_{n\geq 1}$ é de Cauchy em $\mathbb{R}$. Portanto, o teorema 3.16 de [12] garante que $(x_n)_{n\geq 1}$ é convergente, para $x \in \mathbb{R}$, digamos. Analogamente, existe $y \in \mathbb{R}$ tal que $y_n \to y$. Portanto, sendo $z = x + iy$, segue do lema 9.9 que $z_n \to z$. □

Como no caso real (tratado no capítulo 3 de [12]), dada uma sequência $(z_n)_{n\geq 1}$ de números complexos, definimos a série[1] $\sum_{k\geq 1} z_k$ como sendo a sequência $(s_n)_{n\geq 1}$, tal que $s_n = \sum_{k=1}^{n} z_k$, para todo $n \in \mathbb{N}$. Também como lá, dizemos que s_n é a **n−ésima soma parcial** da série, e que a série **converge** se existir o limite $s := \lim_{n\to+\infty} s_n$; ademais, nesse caso dizemos que s é a **soma** da série em questão. Em símbolos, escrevemos

$$\sum_{k\geq 1} z_k = \lim_{n\to+\infty} \sum_{k=1}^{n} z_k,$$

caso o limite do segundo membro exista.

Ilustramos, a seguir, o exemplo de uma série convergente que será de importância fundamental na próxima seção.

[1] Por vezes, consideraremos uma sequência $(z_n)_{n\geq 0}$ de números complexos e a série correspondente $\sum_{k\geq 0} z_k$.

Exemplo 9.12. *Se $a \in \mathbb{C} \setminus \{0\}$, mostre que, para $z \in D(0; \frac{1}{|a|})$, temos*

$$\frac{1}{1-az} = \sum_{k \geq 0} a^k z^k.$$

Prova. Pelo lema 1.12, a $n-$ésima soma parcial da série do enunciado é

$$\sum_{k=0}^{n} (az)^k = \frac{1-(az)^{n+1}}{1-az} = \frac{1}{1-az} - \frac{(az)^{n+1}}{1-az}.$$

Agora, para $z \in D(0; \frac{1}{|a|})$, temos $|az| < 1$, de sorte que, pelo exemplo 9.8, temos $(az)^n \to 0$ quando $n \to +\infty$. Portanto, segue da igualdade acima que, para $z \in D(0; \frac{1}{|a|})$,

$$\sum_{k \geq 0} (az)^k = \lim_{n \to +\infty} \sum_{k=0}^{n} (az)^k = \frac{1}{1-az} - \lim_{n \to +\infty} \frac{(az)^{n+1}}{1-az} = \frac{1}{1-az}.$$

□

Também de fundamental importância é o conceito de **série absolutamente convergente**, i.e., uma série $\sum_{k \geq 0} a_k$ tal que a série real $\sum_{k \geq 0} |a_k|$ converge. Para $n \in \mathbb{N}$, sejam $s_n = \sum_{k=1}^{n} a_k$ e $t_n = \sum_{k=1}^{n} |a_k|$, de sorte que a sequência $(t_n)_{n \geq 1}$ converge. A desigualdade triangular para números complexos fornece, para $m > n$ inteiros,

$$|s_m - s_n| = \left| \sum_{k=n+1}^{m} a_k \right| \leq \sum_{k=n+1}^{m} |a_k| = t_m - t_n.$$

Agora, vimos no capítulo 3 de [12] que, como $(t_n)_{n \geq 1}$ converge, temos $(t_n)_{n \geq 1}$ de Cauchy; portanto, dado $\epsilon > 0$, existe $k_0 \in \mathbb{N}$ tal que $m > n > k_0 \Rightarrow t_m - t_n < \epsilon$. Logo, também temos $|s_m - s_n| < \epsilon$ para $m > n > k_0$, de sorte que $(s_n)_{n \geq 0}$ também é de Cauchy. Como vimos na proposição 9.11 que toda sequência de Cauchy em $\mathbb{C}$ é convergente, o argumento acima prova o resultado a seguir.

Proposição 9.13. *Em $\mathbb{C}$, toda série absolutamente convergente é convergente.*

Antes de continuar, precisamos entender o que vem a ser uma função *contínua* definida e tomando valores em um subconjunto de $\mathbb{C}$.

Definição 9.14. *Dado um subconjunto não vazio X de $\mathbb{C}$, dizemos que uma função $f : X \to \mathbb{C}$ é* **contínua** *se a seguinte condição for satisfeita: para toda sequência $(z_n)_{n \geq 1}$ de pontos de X, se $z_n \to z$, com $z \in X$, então $f(z_n) \to f(z)$.*

A proposição a seguir nos permitirá construir um exemplo de função contínua de nosso interesse.

Proposição 9.15. *Se $f, g : X \to \mathbb{C}$ são funções contínuas, então $f + g, fg : X \to \mathbb{C}$ também são contínuas.*

Prova. Seja dada uma sequência $(z_n)_{n \geq 1}$ em X, tal que $z_n \to z$, com $z \in X$. Observe inicialmente que, pela desigualdade triangular para números complexos,

$$\begin{aligned} |(f+g)(z_n) - (f+g)(z)| &= |(f(z_n) - f(z)) + (g(z_n) - g(z)| \\ &\leq |f(z_n) - f(z)| + |g(z_n) - g(z)|. \end{aligned}$$

Agora, dado $\epsilon > 0$, como $f(z_n) \to f(z)$ e $g(z_n) \to g(z)$, existe $n_0 \in \mathbb{N}$ tal que

$$n > n_0 \Rightarrow |f(z_n) - f(z)|, |g(z_n) - g(z)| < \frac{\epsilon}{2}.$$

Portanto, também para $n > n_0$, segue dos cálculos acima que

$$|(f+g)(z_n) - (f+g)(z)| \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

e, daí, $(f+g)(z_n) \to (f+g)(z)$.

Para fg, e aplicando duas vezes a desigualdade triangular para números complexos, obtemos

$$\begin{aligned}|(fg)(z_n) - (fg)(z)| &= |f(z_n)g(z_n) - f(z)g(z)| \\ &\leq |f(z_n) - f(z)||g(z_n)| + |f(z)||g(z_n) - g(z)| \\ &\leq |f(z_n) - f(z)||g(z_n) - g(z)| \\ &\quad + |f(z_n) - f(z)||g(z)| + |f(z)||g(z_n) - g(z)|.\end{aligned}$$

Como antes, dado $\epsilon > 0$, tome $n_0 \in \mathbb{N}$ tal que $n > n_0$ implique

$$|f(z_n) - f(z)| < \min\left\{\sqrt{\frac{\epsilon}{3}}, \frac{\epsilon}{3(|g(z)| + 1)}\right\}$$

e

$$|g(z_n) - g(z)| < \min\left\{\sqrt{\frac{\epsilon}{3}}, \frac{\epsilon}{3(|f(z)| + 1)}\right\}.$$

Então, para $n > n_0$, segue dos cálculos acima que

$$\begin{aligned}|(fg)(z_n) - (fg)(z)| &\leq \sqrt{\frac{\epsilon}{3}} \cdot \sqrt{\frac{\epsilon}{3}} + \frac{\epsilon}{3(|g(z)| + 1)} \cdot |g(z)| \\ &\quad + |f(z)| \cdot \frac{\epsilon}{3(|f(z)| + 1)} \\ &< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon\end{aligned}$$

e, daí, $(fg)(z_n) \to (fg)(z)$. □

Exemplo 9.16. *Dados $n \in \mathbb{N}$ e $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{C}$, com $a_n \neq 0$, a função polinomial $f : \mathbb{C} \to \mathbb{C}$, tal que*

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0,$$

para $z \in \mathbb{C}$, é contínua.

Prova. Evidentemente, as funções constantes e a função $z \mapsto z$ são contínuas. Portanto, aplicando várias vezes a segunda parte da proposição anterior, concluímos que, para $0 \leq k \leq n$, a função $z \mapsto a_k z^k$ é contínua. Agora, aplicando várias vezes a primeira parte da proposição anterior, concluímos que a soma de tais funções, quando k varia de 0 a n, também é contínua. Mas tal soma é, precisamente, a função f. □

Voltemo-nos, agora, á discussão de *séries de potências* em $\mathbb{C}$. Uma **série de potências** em $\mathbb{C}$ é uma série da forma $\sum_{k\geq 0} a_k z^k$, onde $(a_n)_{n\geq 0}$ é uma sequência dada de números complexos.

Admita que a sequência $(\sqrt[k]{|a_k|})_{k\geq 0}$ é limitada, digamos $\sqrt[k]{|a_k|} < l$, para todo $k \geq 0$ e algum $l > 0$. Então, $|a_k z^k| \leq (lz)^k$ para $k \geq 0$, de sorte que, pelo exemplo 9.12, a série $\sum_{k\geq 0} |a_k z^k|$ converge em $D(0; R)$, onde $R = \frac{1}{l}$. A proposição anterior garante, então, que a série de potências $\sum_{k\geq 0} a_k z^k$ converge em $D(0; R)$. Abreviaremos a situação descrita até aqui dizendo que $D(0; R)$ é um *disco de convergência* para a série de potências em questão. Nosso próximo resultado garante que a função $f : D(0; R) \to \mathbb{C}$ assim definida é contínua. Por uniformidade de notação, convencionamos que $\sum_{k\geq 0} a_k z^k = a_0$ para $z = 0$.

Proposição 9.17. *Se $D(0; R)$ é um disco de convergência para a série de potências $\sum_{k\geq 0} a_k z^k$, então a função $f : D(0; R) \to \mathbb{C}$, dada para $z \in D(0; R)$ por $f(z) = \sum_{k\geq 0} a_k z^k$, é contínua.*

Prova. Sejam $z, w \in D(0; R)$ tais que $|w - z| < \frac{1}{2}(R - |z|)$. Então, $|w| < r$, onde $r = \frac{1}{2}(R + |z|)$ e, para $k \in \mathbb{N}$,

$$\begin{aligned}|w^k - z^k| &= |w - z||w^{k-1} + w^{k-2}z + \cdots + wz^{k-2} + z^{k-1}| \\ &\leq |w - z|(|w|^{k-1} + |w|^{k-2}|z| + \cdots + |w||z|^{k-2} + |z|^{k-1}) \\ &\leq |w - z|(r^{k-1} + r^{k-2} \cdot r + \cdots + r \cdot r^{k-2} + r^{k-1}) \\ &= kr^{k-1}|w - z|.\end{aligned}$$

Portanto, mantida a restrição acima sobre w, segue do problema 4 que

$$\begin{aligned} |f(w) - f(z)| &= \left|\sum_{k\geq 0} a_k w^k - \sum_{k\geq 0} a_k z^k\right| = \left|\sum_{k\geq 0} a_k(w^k - z^k)\right| \\ &= \left|\sum_{k\geq 1} a_k(w^k - z^k)\right| \leq \sum_{k\geq 1} |a_k||w^k - z^k| \\ &\leq \frac{1}{r}\left(\sum_{k\geq 1} k|a_k|r^k\right)|w - z|. \end{aligned}$$

Agora, fixe um real c tal que $1 < c < \frac{R}{r}$ (tal é possível, uma vez que $r < R$). Como $\sqrt[k]{|a_k|} < \frac{1}{R}$ para $k \geq 0$ e $\sqrt[k]{k} \to 1$ (de acordo com o exemplo 3.12 de [12]), existe $k_0 \in \mathbb{N}$ tal que $\sqrt[k]{k|a_k|} < \frac{c}{R}$, para $k > k_0$. Daí,

$$\sum_{k\geq k_0} k|a_k|r^k < \sum_{k\geq k_0}\left(\frac{cr}{R}\right)^k := C < +\infty,$$

uma vez que $0 < \frac{cr}{R} < 1$. Fazendo $C' = \sum_{k=1}^{k_0} k|a_k|r^k$, segue que

$$\begin{aligned} |f(w) - f(z)| &\leq \frac{1}{r}\left(\sum_{k=1}^{k_0} k|a_k|r^k\right)|w - z| + \frac{1}{r}\left(\sum_{k>k_0} k|a_k|r^k\right)|w - z| \\ &\leq \frac{C'}{r}|w - z| + \frac{C}{r}|w - z|. \end{aligned}$$

Em resumo, mostramos que

$$|w - z| < \frac{1}{2}(R - |z|) \Rightarrow |f(w) - f(z)| < A|w - z|,$$

para alguma constante positiva A. Mas, sendo esse o caso, o problema 7 mostra que $z_n \to z \Rightarrow f(z_n) \to f(z)$, e a arbitrariedade de z garante a continuidade de f. $\square$

O corolário a seguir mostra que, se uma função $f : D(0; R) \to \mathbb{C}$ for dada por uma série de potências, então tal série é única.

Corolário 9.18. *Sejam $\sum_{k\geq 0} a_k z^k$ e $\sum_{k\geq 0} b_k z^k$ séries de potências convergentes no disco aberto $D(0; R)$. Se $\sum_{k\geq 0} a_k z^k = \sum_{k\geq 0} b_k z^k$, para todo $z \in D(0; R)$, então $a_k = b_k$, para todo $k \geq 0$.*

Prova. Avaliando a igualdade $\sum_{k\geq 0} a_k z^k = \sum_{k\geq 0} b_k z^k$ para $z = 0$, obtemos $a_0 = b_0$. Então, cancelando $a_0 = b_0$ em ambos os membros da igualdade $\sum_{k\geq 0} a_k z^k = \sum_{k\geq 0} b_k z^k$, obtemos $\sum_{k\geq 1} a_k z^k = \sum_{k\geq 1} b_k z^k$, para $z \in D(0; R)$ e, daí, $\sum_{k\geq 1} a_k z^{k-1} = \sum_{k\geq 1} b_k z^{k-1}$, para $z \in D(0; R) \setminus \{0\}$. Mas, como ambos os membros da última igualdade definem funções contínuas em $D(0; R)$, concluímos que $\sum_{k\geq 1} a_k z^{k-1} = \sum_{k\geq 1} b_k z^{k-1}$, para $z \in D(0; R)$. Então, avaliando essa última igualdade em $z = 0$, obtemos $a_1 = b_1$. Prosseguindo dessa maneira, mostramos indutivamente que $a_k = b_k$, para todo $k \geq 0$. $\square$

Terminamos esta seção com um resultado que estende, para funções contínuas $f : \overline{D(a; R)} \to \mathbb{C}$, o teorema 3.14 de [12].

Teorema 9.19 (Weierstrass). *Se $f : \overline{D(a; R)} \to \mathbb{C}$ é uma função contínua, então existem z_m e z_M em $\overline{D(a; R)}$, tais que*

$$|f(z_m)| = \min\{|f(z)|;\ z \in \overline{D(a; R)}\}$$

e

$$|f(z_M)| = \max\{|f(z)|;\ z \in \overline{D(a; R)}\}.$$

Prova. Seja $(z_n)_{n\geq 1}$ uma sequência em $\overline{D(a; R)}$ tal que

$$f(z_n) \to \sup\{|f(z)|;\ z \in \overline{D(a; R)}\}$$

(aqui, em princípio não excluímos a possibilidade de que tal sup seja $+\infty$). Ponha $z_n = x_n + iy_n$, com $x_n, y_n \in \mathbb{R}$. Como $|z_n| \leq R$ para todo $n \geq 1$, temos $|x_n|, |y_n| \leq R$, para todo $n \geq 1$. Pelo teorema 4.31 de [12], podemos tomar um subconjunto infinito $\mathbb{N}_1 \subset \mathbb{N}$, tal que $(x_n)_{n\in\mathbb{N}_1}$ converge para um certo $x \in \mathbb{R}$. Daí, podemos tomar um segundo subconjunto infinito $\mathbb{N}_2 \subset \mathbb{N}_1$, tal que $(y_n)_{n\in\mathbb{N}_2}$ converge para

um certo $y \in \mathbb{R}$. Mas, como $(x_n)_{n\in\mathbb{N}_2}$ é uma subsequência de $(x_n)_{n\in\mathbb{N}_1}$, temos que $(x_n)_{n\in\mathbb{N}_2}$ ainda converge para x.

Fazendo $z_M = x+iy$, segue do lema 9.9 que $(z_n)_{n\in\mathbb{N}_2}$ converge para z_M. Portanto, segue do problema 1 que $|z_M| \leq R$, i.e., $z_M \in \overline{D(a;R)}$. Invocando agora a continuidade de f, temos que

$$f(z_M) = \lim_{\substack{n\to+\infty \\ n\in\mathbb{N}_2}} f(z_n) = \sup\{|f(z)|;\ z \in \overline{D(a;R)}\}.$$

Em particular, $\sup\{|f(z)|;\ z \in \overline{D(a;R)}\} = \max\{|f(z)|;\ z \in \overline{D(a;R)}\}$.

A prova da primeira parte do teorema é análoga e será deixada como exercício para o leitor. □

Corolário 9.20. *Se $f : \mathbb{C} \to \mathbb{C}$ é uma função polinomial, então, dado $R > 0$, existem z_m e z_M em $\overline{D(a;R)}$, tais que*

$$|f(z_m)| = \min\{|f(z)|;\ z \in \overline{D(a;R)}\}$$

e

$$|f(z_M)| = \max\{|f(z)|;\ z \in \overline{D(a;R)}\}.$$

Prova. O exemplo 9.16 e o problema 6 garantem que $|f| : \mathbb{C} \to [0,+\infty)$ é uma função contínua. Portanto, também é contínua a função $|f| : \overline{D(a;R)} \to [0,+\infty)$. Basta, agora, aplicar o teorema de Weierstrass. □

Problemas – Seção 9.2

1. * Se $(z_n)_{n\geq 1}$ é uma sequência em $\mathbb{C}$ convergindo para $z \in \mathbb{C}$, prove que $(z_n)_{n\geq 1}$ é **limitada**, i.e., que existe $M > 0$ tal que $|z_n| < M$, para todo $n \geq 1$. Ademais, se $|z_n| \leq R$, para todo $n \geq 1$, mostre que $|z| \leq R$.

Para o próximo problema, dizemos que uma sequência de números complexos é **divergente** se não for convergente.

2. Se $|z| > 1$ e $z_n = z^n$, para todo $n \geq 1$, mostre que a sequência $(z_n)_{n\geq 1}$ é divergente.

3. * Se $(z_n)_{n\geq 1}$ e $(w_n)_{n\geq 1}$ são sequências em $\mathbb{C}$, convergindo respectivamente para z e w, prove que:

   (a) Se $a \in \mathbb{C}$, então $az_n \to az$.

   (b) $z_n \pm w_n \to z \pm w$.

   (c) $z_n w_n \to zw$.

   (d) Se $w_n, w \neq 0$, então $z_n/w_n \to z/w$.

4. * Se $a, b \in \mathbb{C}$ e $\sum_{k\geq 1} z_k$ e $\sum_{k\geq 1} w_k$ são séries convergentes de números complexos, mostre que $\sum_{k\geq 1}(az_k + bw_k)$ também é convergente, com

$$\sum_{k\geq 1}(az_k + bw_k) = a\sum_{k\geq 1} z_k + b\sum_{k\geq 1} w_k.$$

5. * Se $\emptyset \neq X \subset Y \subset \mathbb{C}$ e $f : Y \to \mathbb{C}$ é uma função contínua, prove que $f_{|X} : X \to \mathbb{C}$ também é contínua.

6. * Se $\emptyset \neq X \subset \mathbb{C}$ e $f : X \to \mathbb{C}$ é uma função contínua, prove que $|f| : X \to [0,+\infty)$ também é contínua.

7. * Seja $\emptyset \neq X \subset \mathbb{C}$ e $f : X \to \mathbb{C}$ uma função satisfazendo a seguinte condição: para $z \in X$, existem $A, B > 0$ (em princípio dependendo de z), tais que

$$w \in X,\ |w - z| < B \Rightarrow |f(w) - f(z)| < A|w - z|.$$

Mostre que f é contínua.

8. * Se $a \in \mathbb{C} \setminus \{0\}$ e $m \in \mathbb{N}$, mostre que, para $z \in D(0; \frac{1}{|a|})$, temos

$$\frac{1}{(1-az)^m} = \sum_{n \geq 0} \binom{n+m-1}{m-1} a^n z^n.$$

9.3 O caso geral

De posse do material da seção anterior, podemos finalmente nos voltar à discussão do caso geral de (9.1), i.e., aquele em que as raízes complexas do polinômio característico (9.2) não são necessariamente distintas. Para tanto, nos valeremos da teoria de funções geradoras (discutida no capítulo 3 de [13]), adequadamente estendida a séries de potências sobre $\mathbb{C}$.

O resultado fundamental é dado pelo teorema a seguir.

Teorema 9.21. *Seja $(a_n)_{n \geq 1}$ uma sequência satisfazendo, para $n \geq 1$, a recorrência linear*

$$a_{n+k} = u_{k-1}a_{n+k-1} + \cdots + u_0 a_n,$$

onde $u_0, \ldots, u_{k-1}$ são números complexos dados, com $u_0 \neq 0$. Sejam $z_1, \ldots, z_l$ as raízes duas a duas distintas do polinômio característico (9.2) de $(a_n)_{n \geq 1}$, com multiplicidades respectivamente iguais a $m_1, \ldots, m_l$. Então, para $n \geq 1$ temos

$$a_n = p_1(n-1)z_1^{n-1} + \cdots + p_l(n-1)z_l^{n-1},$$

onde $p_1, \ldots, p_l \in \mathbb{C}[X]$ são polinômios de graus menores ou iguais a $m_1 - 1, \ldots, m_l - 1$, respectivamente, os quais são totalmente determinados pelos valores de $a_1, \ldots, a_k$.

Prova. Afirmamos, inicialmente, que existe uma constante $R_0 > 0$ tal que $|a_n| \leq R^n$, para todos $n \geq 1$ e $R > R_0$. De fato, se $|a_n| \leq R^n$

para $1 \leq n < m$, com $m > k$, então

$$\begin{aligned} |a_m| &= |u_{k-1}a_{m-1} + \cdots + u_1 a_{m-k+1} + u_0 a_{m-k}| \\ &\leq |u_{k-1}||a_{m-1}| + \cdots + |u_1||a_{m-k+1}| + |u_0||a_{m-k}| \\ &\leq |u_{k-1}|R^{m-1} + \cdots + |u_1|R^{m-k+1} + |u_0|R^{m-k} \\ &= R^{m-k}(|u_{k-1}|R^{k-1} + \cdots + |u_1|R + |u_0|). \end{aligned}$$

Portanto, se $g(X) = X^k - |u_{k-1}|X^{k-1} - \cdots - |u_1|X - |u_0|$ e $R_0 > 0$ for tal que $g(R) > 0$ para $R > R_0$, então, para cada um de tais R's, temos pelos cálculos acima que

$$\begin{aligned} |a_m| &\leq R^{m-k}(|u_{k-1}|R^{k-1} + \cdots + |u_1|R + |u_0|) \\ &\leq R^{m-k} \cdot R^k = R^m. \end{aligned}$$

Basta, pois, escolhermos, de início, $R_0 > 0$ tal que $|a_1|, \ldots, |a_k| \leq R_0$ e $g(R) > 0$, para todo $R > R_0$.

Agora, fixe $R > R_0$ e seja

$$F(z) = \sum_{n \geq 1} a_n z^n.$$

Como $|a_n| \leq R^n$ para $n \geq 1$, o teste da comparação garante a convergência de F no disco aberto $D(0; \frac{1}{R})$ do plano complexo. Sejam $f(X) = X^k - u_{k-1}X^{k-1} - \cdots - u_1 X - u_0$ o polinômio característico de $(a_n)_{n \geq 1}$ e $h(X) = -u_0 X^k - u_1 X^{k-1} - \cdots - u_{k-1}X + 1$ seu recíproco ($\partial h = k$, uma vez que $u_0 \neq 0$). Para $z \in D(0; \frac{1}{R})$, temos

$$\begin{aligned} h(z)F(z) &= -\left(\sum_{j=0}^{k-1} u_j z^{k-j}\right)\left(\sum_{n \geq 1} a_n z^n\right) + \sum_{n \geq 1} a_n z^n \\ &= -\sum_{j=0}^{k-1} \sum_{n \geq 1} u_j a_n z^{n+k-j} + \sum_{n \geq 1} a_n z^n \\ &= -\sum_{j=0}^{k-1} \sum_{n \geq k-j+1} u_j a_{n-k+j} z^n + \sum_{n \geq 1} a_n z^n. \end{aligned}$$

Para $j \geq 2$, escreva

$$\sum_{n\geq k-j+1} u_j a_{n-k+j} z^n = \sum_{n=k-j+1}^{k-1} u_j a_{n-k+j} z^n + \sum_{n\geq k} u_j a_{n-k+j} z^n$$

e analogamente para $\sum_{n\geq 1} a_n z^n$. Obtemos

$$\begin{aligned} h(z)F(z) &= -\sum_{n\geq k+1} u_0 a_{n-k} z^n - \sum_{n\geq k} u_1 a_{n-k+1} z^n \\ &\quad - \sum_{j=2}^{k-1}\left(\sum_{n=k-j+1}^{k-1} u_j a_{n-k+j} z^n + \sum_{n\geq k} u_j a_{n-k+j} z^n\right) \\ &\quad + \sum_{n=1}^{k-1} a_n z^n + \sum_{n\geq k} a_n z^n \\ &= -\sum_{n\geq k+1} u_0 a_{n-k} z^n - \sum_{n\geq k} u_1 a_{n-k+1} z^n \\ &\quad - \sum_{j=2}^{k-1}\sum_{n\geq k} u_j a_{n-k+j} z^n + \sum_{n\geq k} a_n z^n \\ &\quad - \sum_{j=2}^{k-1}\sum_{n=k-j+1}^{k-1} u_j a_{n-k+j} z^n + \sum_{n=1}^{k-1} a_n z^n. \end{aligned}$$

Mas, como

$$\sum_{j=2}^{k-1}\sum_{n\geq k} u_j a_{n-k+j} z^n = \sum_{n\geq k}\sum_{j=2}^{k-1} u_j a_{n-k+j} z^n,$$

segue de (9.1) que

$$\begin{aligned} -\sum_{j=2}^{k-1}\sum_{n\geq k} u_j a_{n-k+j} z^n + \sum_{n\geq k} a_n z^n &= \sum_{n\geq k}\left(-\sum_{j=2}^{k-1} u_j a_{n-k+j} + a_n\right) z^n \\ &= \left(-\sum_{j=2}^{k-1} u_j a_j + a_k\right) z^k + \sum_{n\geq k+1}\left(-\sum_{j=2}^{k-1} u_j a_{n-k+j} + a_n\right) z^n \\ &= \left(-\sum_{j=2}^{k-1} u_j a_j + a_k\right) z^k + \sum_{n\geq k+1} (u_0 a_{n-k} + u_1 a_{n-k+1}) z^n. \end{aligned}$$

Portanto,

$$\begin{aligned} h(z)F(z) &= -\sum_{n\geq k+1} u_0 a_{n-k} z^n - \sum_{n\geq k} u_1 a_{n-k+1} z^n \\ &\quad + \left(-\sum_{j=2}^{k-1} u_j a_j + a_k\right) z^k + \sum_{n\geq k+1} (u_0 a_{n-k} + u_1 a_{n-k+1}) z^n \\ &\quad - \sum_{j=2}^{k-1}\sum_{n=k-j+1}^{k-1} u_j a_{n-k+j} z^n + \sum_{n=1}^{k-1} a_n z^n \\ &= \left(a_k - \sum_{j=1}^{k-1} u_j a_j\right) z^k - \sum_{j=2}^{k-1}\sum_{n=k-j+1}^{k-1} u_j a_{n-k+j} z^n + \sum_{n=1}^{k-1} a_n z^n, \end{aligned}$$

de sorte que

$$h(z)F(z) = zp(z)$$

para $z \in D(0; \frac{1}{R})$, onde $p \in \mathbb{C}[X]$ é um polinômio não nulo, de grau $\partial p \leq k-1$.

Como $h(0) = 1 \neq 0$, aumentando R, se necessário, podemos supor que $h(z) \neq 0$ para $z \in D(0; \frac{1}{R})$. Por outro lado, como

$$f(X) = (X - z_1)^{m_1} \ldots (X - z_l)^{m_l},$$

temos

$$h(X) = (1 - z_1 X)^{m_1} \ldots (1 - z_l X)^{m_l},$$

de sorte que

$$F(z) = \frac{zp(z)}{(1-z_1z)^{m_1}\dots(1-z_lz)^{m_l}}, \tag{9.6}$$

para $z \in D(0; \frac{1}{R})$.

Agora, observe que

$$\partial p < k = \partial((1-z_1z)^{m_1}\dots(1-z_lz)^{m_l}).$$

Portanto, aplicando à igualdade (9.6) a fórmula de decomposição em frações parciais (conforme o problema 6, página 163), concluímos pela existência, para $1 \leq j \leq l$ e $1 \leq n_j \leq m_j$, de constantes d_{jn_j}, unicamente determinadas pelos coeficientes de p (e, portanto, por a_1, a_2, $\dots$, a_k e u_0, u_1, $\dots$, u_{k-1}), tais que

$$F(z) = z\sum_{j=1}^{l}\sum_{n_j=1}^{m_j}\frac{d_{jn_j}}{(1-z_jz)^{n_j}}, \tag{9.7}$$

para $z \in D(0; \frac{1}{R})$.

Mas, se $r = \min\{\frac{1}{R}, \frac{1}{|z_1|}, \dots, \frac{1}{|z_l|}\}$, então o resultado do problema 8, página 234, garante que

$$\frac{1}{(1-z_jz)^{n_j}} = \sum_{n\geq 0}\binom{n+n_j-1}{n_j-1}z_j^nz^n,$$

para $1 \leq j \leq l$, $1 \leq n_j \leq m_j$ e $z \in D(0;r)$. Portanto, segue de (9.7) que, para $|z| < r$,

$$\begin{aligned} F(z) &= z\sum_{j=1}^{l}\sum_{n_j=1}^{m_j}\sum_{n\geq 0} d_{jn_j}\binom{n+n_j-1}{n_j-1}z_j^nz^n \\ &= \sum_{n\geq 0}\left(\sum_{j=1}^{l}\sum_{n_j=1}^{m_j} d_{jn_j}\binom{n+n_j-1}{n_j-1}z_j^n\right)z^{n+1} \\ &= \sum_{n\geq 1}\left(\sum_{j=1}^{l}\sum_{n_j=1}^{m_j} d_{jn_j}\binom{n+n_j-2}{n_j-1}z_j^{n-1}\right)z^n. \end{aligned}$$

Uma vez que a_n é o coeficiente de z^n na série que define F, segue da última igualdade acima e do corolário 9.18 que

$$\begin{aligned} a_n &= \sum_{j=1}^{l}\sum_{n_j=1}^{m_j} d_{jn_j}\binom{n+n_j-2}{n_j-1}z_j^{n-1} \\ &= \sum_{j=1}^{l}\sum_{n_j=1}^{m_j}\frac{d_{jn_j}}{(n_j-1)!}(n+n_j-2)(n+n_j-3)\dots(n+1)nz_j^{n-1} \\ &= \sum_{j=1}^{l}p_j(n-1)z_j^{n-1}, \end{aligned}$$

onde

$$\begin{aligned} p_j(X) &= \sum_{n_j=1}^{m_j}\frac{d_{jn_j}}{(n_j-1)!}(X+n_j-1)(X+n_j-2)\dots(X+1)z_j^{n-1} \\ &= c_{j,m_j-1}X^{m_j-1}+\dots+c_{j1}X+c_{j0}, \end{aligned}$$

um polinômio de grau menor ou igual a $m_j - 1$. □

A fim de apresentar uma aplicação relevante do teorema anterior, precisamos da seguinte definição.

Definição 9.22. *Sejam dados uma sequência* $(a_n)_{n\geq 1}$ *e um inteiro* $m > 1$. *Dizemos que* $(a_n)_{n\geq 1}$ *é uma*

(a) **PA de ordem 1** *se* $(a_n)_{n\geq 1}$ *for uma PA.*

(b) **PA de ordem m** *se a sequência* $(b_n)_{n\geq 1}$ *for uma PA de ordem* $m-1$, *onde* $b_n = a_{n+1} - a_n$, *para* $n \geq 1$.

O lema a seguir caracteriza PA's de ordem m por meio de uma recorrência linear que generaliza a recorrência satisfeita pelas PA's ordinárias.

Lema 9.23. *Uma sequência* $(a_n)_{n\geq 1}$ *é uma PA de ordem* m *se, e só se,*

$$\binom{m+1}{0}a_{n+m+1} - \binom{m+1}{1}a_{n+m} + \cdots + (-1)^{m+1}\binom{m+1}{m+1}a_n = 0, \tag{9.8}$$

para todo $n \geq 1$.

Prova. Inicialmente, seja $(a_n)_{n\geq 1}$ uma PA de ordem m. Se $m = 1$, então $(a_n)_{n\geq 1}$ é uma PA e (9.8) se reduz a $a_{n+2} - 2a_{n+1} + a_n = 0$ para $n \geq 1$, relação que sabemos ser sempre satisfeita por uma PA. Por hipótese de indução, suponha que (9.8) é válida quando $m = k - 1$. Para $m = k$, a sequência $(b_n)_{n\geq 1}$, dada por $b_n = a_{n+1} - a_n$ é, por definição, uma PA de ordem $k - 1$. Portanto, segue da hipótese de indução que

$$\binom{k}{0}b_{n+k} - \binom{k}{1}b_{n+k-1} + \cdots + (-1)^k\binom{k}{k}b_n = 0, \tag{9.9}$$

para todo $n \geq 1$, ou, ainda,

$$\begin{aligned}\binom{k}{0}(a_{n+k+1} - a_{n+k}) - \binom{k}{1}(a_{n+k} - a_{n+k-1}) + \cdots \\ \cdots + (-1)^k\binom{k}{k}(a_{n+1} - a_n) = 0,\end{aligned} \tag{9.10}$$

para todo $n \geq 1$. Mas, isso é o mesmo que

$$\begin{aligned}\binom{k}{0}a_{n+k+1} - \left(\binom{k}{0} + \binom{k}{1}\right)a_{n+k} + \left(\binom{k}{1} + \binom{k}{2}\right)a_{n+k-1} - \cdots \\ \cdots + (-1)^k\left(\binom{k}{k-1} + \binom{k}{k}\right)a_{n+1} + (-1)^{k+1}\binom{k}{k}a_n = 0,\end{aligned} \tag{9.11}$$

A partir daí, a relação (9.8) para $m = k$ segue da relação de Stifel, juntamente com o fato de que $\binom{k}{0} = \binom{k+1}{0}$ e $\binom{k}{k} = \binom{k+1}{k+1}$.

Reciprocamente, seja $(a_n)_{n\geq 1}$ uma sequência para a qual vale (9.8). Se $m = 1$, então $a_{n+2} - 2a_{n+1} + a_n = 0$ para $n \geq 1$, de sorte que $(a_n)_{n\geq 1}$ é uma PA. Por hipótese de indução, suponha que a validade de (9.8) para $m = k - 1$ acarreta que $(a_n)_{n\geq 1}$ é uma PA de ordem $k-1$. Considere, então, uma sequência $(a_n)_{n\geq 1}$ que satisfaz (9.8) para $m = k$, i.e., tal que

$$\binom{k+1}{0}a_{n+k+1} - \binom{k+1}{1}a_{n+k} + \cdots + (-1)^{k+1}\binom{k+1}{k+1}a_n = 0,$$

para $n \geq 1$. Então, utilizando a relação de Stifel, juntamente com as igualdades $\binom{k+1}{0} = \binom{k}{0}$ e $\binom{k+1}{k+1} = \binom{k}{k}$, reobtemos sucessivamente as relações (9.11), (9.10) e (9.9), para $n \geq 1$. Portanto, segue da hipótese de indução que a sequência $(b_n)_{n\geq 1}$ é uma PA de ordem $k-1$, de sorte que, por definição, $(a_n)_{n\geq 1}$ é uma PA de ordem k. □

Podemos, finalmente, apresentar a aplicação prometida do teorema 9.21.

Exemplo 9.24. *Se* $(a_n)_{n\geq 1}$ *é uma PA de ordem* m, *então* (9.8) *vale para todo* $n \geq 1$, *de sorte que o polinômio característico de* $(a_n)_{n\geq 1}$ *é*

$$\begin{aligned}f(X) &= \binom{m+1}{0}X^{m+1} - \binom{m+1}{1}X^m + \cdots + (-1)^{m+1}\binom{m+1}{m+1} \\ &= (X-1)^{m+1}.\end{aligned}$$

Pelo teorema 9.21, existem constantes $\alpha_0, \alpha_1, \ldots, \alpha_m$ *tais que*

$$a_n = \alpha_0 + \alpha_1(n-1) + \cdots + \alpha_m(n-1)^m,$$

para todo $n \geq 1$. *Avaliando a relação acima para* $n = 1$, *obtemos* $\alpha_0 = a_1$; *avaliando-a para* $n = 2, \ldots, m+1$, *obtemos* $\alpha_1, \ldots, \alpha_m$ *como soluções do sistema linear de equações*

$$\begin{cases} \alpha_1 + \alpha_2 + \cdots + \alpha_m & = & a_2 - a_1 \\ 2\alpha_1 + 2^2\alpha_2 + \cdots + 2^m\alpha_m & = & a_3 - a_1 \\ \cdots & & \cdots \\ m\alpha_1 + m^2\alpha_2 + \cdots + m^m\alpha_m & = & a_{m+1} - a_1 \end{cases}.$$

Observe que o fato de um tal sistema linear de equações sempre admitir uma única solução é uma decorrência imediata do teorema 9.21.

Problemas – Seção 9.3

1. Seja k um natural dado e $(a_n)_{n\geq 1}$ uma sequência tal que

$$a_n = \frac{1}{2}(a_{n-k} + a_{n+k}),$$

para todo natural $n > k$. Use o teorema 9.21 para mostrar que

$$a_n = \sum_{j=1}^{k}(A_j + (n-1)B_j)\omega^{j-1},$$

para todo $n \geq 1$, onde $\omega = \text{cis}\,\frac{2\pi}{k}$.

2. Prove as identidades da proposição 4.17 com o uso de funções geradoras.

CAPÍTULO 10

Soluções e Sugestões

Seção 1.1

2 Para o item (b), escreva $|z+w|^2 = (z+w)(\overline{z+w})$ e use o resultado do item (b) do lema 1.1, juntamente com 1.8.

3. Para o item (a), aplique a desigualdade $|z+w| \leq |z|+|w|$, com $u-z$ no lugar de z e $z-v$ no lugar de w. Para o item (b), observe que a desigualdade em questão é equivalente a $-|z-w| \leq |z|-|w| \leq |z-w|$; em seguida, para obter a desigualdade $|z|-|w| \leq |z-w|$, aplique a desigualdade $|z+w| \leq |z|+|w|$, escrevendo $z-w$ no lugar de z.

4. Se z tem a forma do enunciado, use o item (a) do problema 2 para concluir que $|z| = 1$. Reciprocamente, suponha que $|z| = 1$. Imponha que $z = \frac{1-iw}{1+iw}$, com $w \in \mathbb{C}$, para obter $w = i\frac{1-z}{1+z}$; em seguida, use os itens (b) e (d) do lema 1.1, juntamente com o fato de que $|z| = 1$, para concluir que $w \in \mathbb{R}$.

5. Desenvolva ambos os membros da desigualdade $|z-a|^2 < |1-\overline{a}z|^2$, utilizando o resultado do item (b) do problema 2.

6. Note inicialmente que $z_{k+1} = z_k\left(1+\frac{i}{\sqrt{k+1}}\right)$. Em seguida, calcule $|z_k|$ em função de k utilizando produtos telescópicos. Por fim, veja que $z_{k+1} - z_k = \frac{z_k i}{\sqrt{k+1}}$.

7. Revise a definição de adição e subtração de vetores, no capítulo 8 de [11].

8. Suponha que uma tal ordem total exista e chegue a uma contradição.

9. As verificações dos itens (a) a (e) são longas, mas elementares. Quanto ao item (f), a primeira parte é imediata a partir da definição da multiplicação em $\mathbb{H}$; para a segunda parte, basta utilizar a igualdade $|\alpha\beta|^2 = \alpha\beta\overline{\alpha\beta}$, juntamente com o resultado do item (e). O item (g) segue da segunda parte de (f). Finalmente, se $\alpha \in \mathbb{H}\setminus\{0\}$, então $\alpha\cdot\frac{\overline{\alpha}}{|\alpha|^2} = 1$; daí, se $\alpha\beta = 0$ e $\alpha \neq 0$, então
$$0 = \frac{\overline{\alpha}}{|\alpha|^2}(\alpha\beta) = \left(\frac{\overline{\alpha}}{|\alpha|^2}\alpha\right)\beta = 1\cdot\beta = \beta.$$
Por fim, se $\alpha\beta = 1$, então $\alpha\beta - \alpha\frac{\overline{\alpha}}{|\alpha|^2} = 0$ ou, ainda, $\alpha\left(\beta - \frac{\overline{\alpha}}{|\alpha|^2}\right) = 0$; mas, como $\alpha \neq 0$, segue que $\beta = \frac{\overline{\alpha}}{|\alpha|^2}$ (aqui, escrevemos $\alpha - \beta$ para denotar $\alpha + (-\beta)$, onde $-\beta = (-w) + (-x)i + (-y)j + (-z)k$ se $\beta = w + xi + yj + zk$).

10. No plano complexo, sejam a, b, c, d e e os números associados aos vértices de $\mathcal{P}$ e suponha, sem perda de generalidade, que $l_{10} = |b-c|$. Em seguida, use um argumento geométrico para mostrar que podemos supor que $d = 0$ e $e = 1$. Em seguida, observe que as condições do enunciado equivalem a que $|a|^2$, $|b|^2$, $|c|^2$, $|a-1|^2$, $|b-1|^2$, $|c-1|^2$, $|a-b|^2$ e $|a-c|^2$ sejam todos racionais. Conclua, com o auxílio do problema 2, que $\mathrm{Re}(a)$, $\mathrm{Re}(b)$, $\mathrm{Re}(c)$, $\mathrm{Re}(a\overline{b})$ e $\mathrm{Re}(a\overline{c})$ são racionais e, também, que $\mathrm{Im}(a)^2 = |a|^2 - \mathrm{Re}(a)^2$ é racional. Como
$$\begin{aligned}\mathrm{Re}(a\overline{b}) &= \mathrm{Re}(a)\mathrm{Re}(\overline{b}) - \mathrm{Im}(a)\mathrm{Im}(\overline{b})\\ &= \mathrm{Re}(a)\mathrm{Re}(b) + \mathrm{Im}(a)\mathrm{Im}(b),\end{aligned}$$
deduza que $\mathrm{Im}(a)\mathrm{Im}(b)$ é racional; analogamente, $\mathrm{Im}(a)\mathrm{Im}(c)$ também é racional. Agora, como (novamente pelo problema 2) $|b-c|^2 = |b|^2 + |c|^2 - 2\mathrm{Re}(b\overline{c})$, basta mostrarmos que $\mathrm{Re}(b\overline{c})$ é racional. Para tanto, veja que
$$\mathrm{Re}(b\overline{c}) = \mathrm{Re}(b)\mathrm{Re}(c) + \mathrm{Im}(b)\mathrm{Im}(c),$$
de sorte que basta mostrarmos que $\mathrm{Im}(b)\mathrm{Im}(c)$ é racional. Para o que falta, escreva
$$\mathrm{Im}(b)\mathrm{Im}(c) = \frac{\mathrm{Im}(a)\mathrm{Im}(b)\cdot\mathrm{Im}(a)\mathrm{Im}(c)}{\mathrm{Im}(a)^2}.$$

Seção 1.2

1. Adapte, ao presente caso, a prova do corolário 1.7.

2. Comece observando que $\omega + \frac{1}{\omega} = -1$ e $\omega^{3k} = 1$, $\omega^{3k+1} = \omega$ e $\omega^{3k+2} = \omega^2$, para todo $k \in \mathbb{Z}$.

3. Ponha $1\pm\sqrt{3}i$ em forma polar e use a primeira fórmula de de Moivre.

4. Conjugue a segunda equação para obter $\overline{z}_1+\overline{z}_2+\overline{z}_3 = 0$. Em seguida, use a primeira equação e o item (d) do lema 1.1 para concluir que $\frac{1}{z_1}+\frac{1}{z_2}+\frac{1}{z_3} = 0$ e, daí, que $z_1z_2 + z_1z_3 + z_2z_3 = 0$. Por fim, observe que $0 = z_1(z_1z_2 + z_1z_3 + z_2z_3) = z_1^2(z_2+z_3) + 1 = -z_1^3 + 1$, valendo identidades análogas para z_2 e z_3.

5. Adapte, ao presente caso, a solução do exemplo 1.11. Para tanto, comece mostrando que a equação dada equivale a $\left(\frac{1+z}{1-z}\right)^{2n} = -1$.

6. Adapte, ao presente caso, a solução do exemplo 1.11, consoante a sugestão dada ao problema anterior.

7. Escreva $a_n = (n-\omega)(n-\omega^2)$, com $\omega = \mathrm{cis}\,\frac{2\pi}{3}$. Em seguida, recorde que $1+\omega+\omega^2 = 0$, de maneira que $(k-1-\omega)(k-\omega^2) = (k+\omega^2)(k-\omega^2) = k^2-\omega$ e, analogamente, $(k-1-\omega^2)(k-\omega) = (k+\omega)(k-\omega) = k^2-\omega^2$.

8. Pondo $w^2 = p^2 - 4q^2$, use a fórmula de Báskara para mostrar que as raízes têm módulos iguais se, e só se, $\mathrm{Re}(\overline{p}w) = 0$; em seguida, substitua $p = r \,\mathrm{cis}\, \alpha$, $q = s \,\mathrm{cis}\, \beta$ e $w = t \,\mathrm{cis}\, \gamma$ em $\omega^2 = p^2 - 4q^2$, com $r, s, t \in \mathbb{R}_+$, e conclua que $|\alpha - \beta|$ é um múltiplo inteiro de π.

9. Fazendo $z_2 = z_2' + z_1$ e $z_3 = z_3' + z_1$, mostre que podemos supor $z_1 = 0$; em seguida, fazendo $z_2'' = wz_2'$ e $z_3'' = wz_3'$, mostre que podemos supor $z_2' = 1$.

10. Se $\omega = \mathrm{cis}\, \frac{2\pi}{n}$, use a primeira fórmula de de Moivre para calcular as partes real e imaginária do primeiro membro de (1.19).

11. Para o item (a), adapte a sugestão dada ao problema anterior. Faça o mesmo quanto ao item (b), utilizando também a fórmula $\mathrm{sen}^2 x = \frac{1}{2}(1 - \cos(2x))$.

12. Para $k \in \mathbb{N}$ fixado, o conjunto das raízes $n-$ésimas da unidade é um subconjunto *finito* de $\mathbb{C}$ satisfazendo as condições (a) e (b).

13. Comece utilizando a finitude de A para mostrar que todos os seus elementos são raízes da unidade. Em seguida, se $z \in A$ e $z^k = 1$ para algum natural k, mostre que $k \mid n$.

14. Opere duas vezes a substituição $z \mapsto \omega z + a$ na condição do enunciado.

Seção 2.1

2. Para o item (c), lembre-se de que, de acordo com o exemplo 5.12 de [10], todo número natural pode ser escrito, de maneira única a menos de uma reordenação, como uma soma de potências de 2, com expoentes inteiros não negativos e dois a dois distintos.

4. Por contraposição, mostre que se $f, g \in K[X] \setminus \{0\}$, então $fg \neq 0$. Para tanto, escreva $f(X) = \sum_{i=k}^{m} a_i X^i$ e $g(X) = \sum_{j=l}^{n} b_j X^j$, com $a_k, b_l \neq 0$, e examine o coeficiente de X^{k+l} em fg.

5. Se $g(X) = f(X) + \frac{1}{2}$, então $g(X) + g(1 - X) = 0$ ou, ainda, $g(X) = -g(1 - X)$. Fazendo $g(X) = (X - a)^{2001}$, devemos ter $(X - a)^{2001} = -(1 - X - a)^{2001} = (X + a - 1)^{2001}$. Basta, pois, escolher a de tal forma que $a = 1 - a$, i.e., $a = \frac{1}{2}$.

Seção 2.2

1. Comece escrevendo $X^2 + X + 1 = (X^2 - X + 1) + 2X$.

2. Comece observando que

$$\begin{aligned} X^{2^m} - 1 &= (X^{2^{m-1}} + 1)(X^{2^{m-1}} - 1) \\ &= (X^{2^{m-1}} + 1)(X^{2^{m-2}} + 1)(X^{2^{m-2}} - 1) = \cdots, \end{aligned}$$

de sorte que $X^{2^n} + 1$ divide $X^{2^m} - 1$.

3. Escreva $f(X) = (X + 2)q_1(X) - 1 = (X - 2)q_2(X) + 3$, com $q_1, q_2 \in \mathbb{Q}[X]$. Em seguida, se $q_1(X) = (X - 2)q(X) + r$, então $f(X) = (X^2 - 4)q(X) + (X + 2)r - 1$. Use a parte de unicidade do algoritmo da divisão para concluir que $r = 1$.

4. Escreva $f(X) = (X + 1)(X^2 + 1)q(X) + (aX^2 + bX + c)$, para certos $a, b, c \in \mathbb{R}$. Em seguida, mostre que os restos das divisões de $aX^2 + bX + c$ por $X + 1$ e $X^2 + 1$ são respectivamente iguais aos polinômios $a - b + c$ e $bX + (c - a)$.

Seção 3.1

1. Inicialmente, mostre que é suficiente considerar o caso em que f é da forma $f(X) = aX^n$, para algum $a \in K \setminus \{0\}$, e g não é constante. Para o que falta, use o corolário 3.14.

2. Para o item (a), use a fórmula do binômio de Newton; para (b), escreva $f(X) = c_nX^n + \cdots + c_1X + c_0$ e use (a) para concluir pela existência de racionais A e B tais que $f(a \pm b\sqrt{r}) = A \pm B\sqrt{r}$. Em seguida, aplique o resultado do problema 1.3.3 de [10].

3. Use o resultado do problema anterior para concluir que o polinômio dado é divisível por $X^2 - 2X - 1$.

4. Use o algoritmo da divisão.

5. Comece observando que, se um tal f existir, então $f(y)^2 = 1 - y^2$, para todo $0 \leq y \leq 1$ e, daí, para todo $y \in \mathbb{R}$. Em seguida, conclua que $\partial f = 1$ e chegue a uma contradição.

6. Use o teste da raiz para $\pm i$.

7. Se a fosse uma raiz inteira de f, use a condição $f(0)$ ímpar, juntamente com o critério de pesquisa de raízes racionais, para concluir que a seria ímpar. Em seguida, mostre que se x for ímpar, então $f(x)$ e $f(1)$ têm paridades iguais, de sorte que $f(a)$ seria ímpar e, portanto, não poderíamos ter $f(a) = 0$.

8. Sendo r a razão da PA, escreva $x = y - r$ e $z = y + r$ e conclua que o polinômio $X^5 - 10X^4 - 20X^2 - 2$ tem a raiz racional x/r. Em seguida, aplique o critério de pesquisa de raízes racionais para chegar a uma contradição.

9. Uma vez que $\{2\cos\theta;\ \theta \in \mathbb{R}\} = [-2, 2]$, o qual é um conjunto infinito, o corolário 3.10 garante que há, no máximo, um polinômio f_n satisfazendo a condição do enunciado. Agora, para o item (a), é imediato verificar que $f_1(X) = X$ e (com o auxílio de um pouco de trigonometria) $f_2(X) = X^2 - 1$ satisfazem as condições do enunciado. Para o que falta, seja $(f_n)_{n\geq 1}$ a sequência de polinômios tal que $f_1(X) = X$, $f_2(X) = X^2 - 1$ e $f_{k+2}(X) = Xf_{k+1}(X) - f_k(X)$, para $k \geq 1$ inteiro. Suponha, por hipótese de indução, que $f_j(2\cos\theta) = 2\cos(j\theta)$, para $1 \leq j \leq k+1$ e todo $\theta \in \mathbb{R}$. Com um pouco de trigonometria, é

imediato verificar que

$$2\cos\theta \cdot 2\cos(k+1)\theta - 2\cos(k\theta) = 2\cos(k+2)\theta$$

ou, o que é o mesmo,

$$\begin{aligned} f_{k+2}(2\cos\theta) &= 2\cos\theta \cdot f_{k+1}(2\cos\theta) - f_k(2\cos\theta) \\ &= 2\cos\theta \cdot 2\cos(k+1)\theta - 2\cos(k\theta) \\ &= 2\cos(k+2)\theta, \end{aligned}$$

para todo $\theta \in \mathbb{R}$. Por fim, (b) e (c) seguem imediatamente de (a), por indução sobre $n \in \mathbb{N}$.

10. Sejam $m, n, p, q \in \mathbb{Z}$, tais que $n, q \neq 0$ e $\cos(\frac{m}{n}\pi) = \frac{p}{q}$. Use o resultado do problema anterior para mostrar que $f_n(\frac{2p}{q}) = 2(-1)^m$ e, daí, que $\frac{2p}{q}$ é raiz de um polinômio mônico e de coeficientes inteiros. Por fim, como $\frac{2p}{q} = 2\cos(\frac{m}{n}\pi) \in [-2, 2]$, conclua que $\frac{p}{q} = 0, \pm\frac{1}{2}$ ou ± 1.

11. Suponha que o polinômio em questão possui uma raiz inteira, r digamos, de sorte que

$$r^4 - 1994r^3 + (1993 + m)r^2 - 11r + m = 0.$$

Examinando tal igualdade módulo 2, conclua que m e r são pares. Suponha, agora, que a e b sejam raízes inteiras distintas do polinômio em questão. Então, subtraindo membro a membro as igualdades

$$a^4 - 1994a^3 + (1993 + m)a^2 - 11a + m = 0$$

e

$$b^4 - 1994b^3 + (1993 + m)b^2 - 11b + m = 0,$$

e fatorando $a - b$ do resultado, obtenha

$$(a + b)(a^2 + b^2) - 1994(a^2 + ab + b^2) + (1993 + m)(a + b) = 11$$

e chegue a uma contradição.

12. Seja $X^2-X-1=(X-u)(X-v)$. Pelo teste da raiz, basta encontrarmos todos os a e b tais que $au^{17}+bu^{16}+1=0$ e $av^{17}+bv^{16}+1=0$. Multiplicando a primeira relação por u^{16}, a segunda por v^{16} e subtraindo os resultados, obtenha $a=\frac{u^{16}-v^{16}}{u-v}$. Agora, defina $x_n=\frac{u^n-v^n}{u-v}$ e mostre que $x_1=x_2=1$ e $x_{n+2}=x_{n+1}+x_n$, para todo $n\in\mathbb{N}$, de sorte que a sequência $(x_n)_{n\geq 1}$ é a sequência de Fibonacci. Conclua, a partir daí, que $a=987$ e calcule o valor de b de modo análogo.

13. Escreva $p(X)=X(X-\alpha_2)\ldots(X-\alpha_n)$, com $\alpha_2,\ldots,\alpha_n$ inteiros não nulos e dois a dois distintos. Para $d\in\mathbb{Z}$, mostre que $p(p(d))=0$ se, e só se, $d=\alpha_i$ para algum $1\leq i\leq n$ ou $p(d)=\alpha_i$, para algum $2\leq i\leq n$. Neste último caso, temos $d\neq 0$; ademais, escrevendo $\alpha=\alpha_i$, mostre que existe $q\in\mathbb{Z}^*$ tal que $d(d-\alpha)q=\alpha$. Conclua que $dq+1=-1$ e, daí, que $d=\frac{\alpha}{2}$. Por fim, deduza, a partir daí, que $(d-\alpha_2)\ldots(d-\alpha_n)=2$, e use o fato de ser $n>4$ para chegar a uma contradição.

14. Há dois casos essencialmente distintos, quais sejam, $f(p_1)=f(p_2)=f(p_3)=3$ e $f(p_4)=-3$, ou $f(p_1)=f(p_2)=3$ e $f(p_3)=f(p_4)=-3$. No primeiro caso, mostre que $f(X)=a(X-p_1)(X-p_2)(X-p_3)+3$ e use, em seguida, a condição $f(p_4)=-3$, juntamente com o fato de os p_i's serem primos e distintos, para chegar a uma contradição. No segundo caso, mostre que $f(X)=a(X-p_1)(X-p_2)(X-q)+3$ e calcule $f(0)$ para concluir que $q=\frac{3-d}{ap_1p_2}$; use, em seguida, as condições $f(p_3)=f(p_4)=-3$ para chegar a uma contradição.

15. Use o teste da raiz para concluir que $p(X)=5+(X-a)(X-b)(X-c)(X-d)q(X)$, para algum polinômio $q\in\mathbb{Z}[X]$; em seguida, faça $x=m$ nas funções polinomiais correspondentes e chegue a uma contradição.

16. Se $\omega=\text{cis}\,\frac{2\pi}{3}$, então ω e ω^2 são raízes cúbicas da unidade e as raízes de X^2+X+1; use tais fatos para examinar para quais $k\in\mathbb{N}$ temos $\omega^{2k}+1+(\omega+1)^{2k}=0$ e, analogamente, para ω^2 no lugar de ω.

17. Comece definindo $f(X)=\sum_{i=1}^n X^{a_i}$ e $g(X)=\sum_{i=1}^n X^{b_i}$; em seguida, use as condições do enunciado para mostrar que 1 é raiz de $f-g$ e que $(f(X)+g(X))(f(X)-g(X))=f(X^2)-g(X^2)$.

Seção 3.2

1. Adapte, ao presente caso, a demonstração do teorema 3.21.

2. Adapte, ao presente caso, a demonstração do teorema 3.21.

3. Use o resultado do problema anterior.

4. Aplique a fórmula de multiseção.

5. Argumentemos como na prova do teorema 3.22: se $f(X)=\sum_{k\geq 0}a_kX^k$ e S denota o segundo membro da expressão do enunciado, então

$$\begin{aligned} S &= \frac{1}{p}\sum_{j=0}^{p-1}\omega^{(p-1)rj}\sum_{k\geq 0}a_k\omega^{jk} \\ &= \frac{1}{p}\sum_{j=0}^{p-1}\sum_{k\geq 0}a_k\omega^{((p-1)r+k)j} \\ &= \frac{1}{p}\sum_{k\geq 0}a_k\sum_{j=0}^{p-1}\omega^{(k-r)j}, \end{aligned}$$

onde utilizamos a relação $\omega^p=1$ na última igualdade. Agora, se $k\equiv r\,(\text{mod}\,p)$, digamos $k-r=pq$, então

$$\sum_{j=0}^{p-1}\omega^{(k-r)j}=\sum_{j=0}^{p-1}(\omega^p)^q=\sum_{j=0}^{p-1}1^q=p;$$

se $k\not\equiv r\,(\text{mod}\,p)$, então $\omega^{k-r}\neq 1$ e, pelo lema 1.12, temos

$$\sum_{j=0}^{p-1}\omega^{(k-r)j}=\frac{\omega^{(k-r)p}-1}{\omega^{k-r}-1}=0.$$

Portanto,

$$S = \frac{1}{p} \sum_{k \equiv r \, (\mathrm{mod}\, p)} a_k p = \sum_{k \equiv r \, (\mathrm{mod}\, p)} a_k.$$

6. Use o resultado do problema anterior.

Seção 3.3

1. Reveja a dedução da fórmula de Báskara, em [10].

2. Conjugue ambos os membros da igualdade $f(z) = 0$. Em seguida, escreva $f(z) = a_n z^n + \cdots + a_1 z + a_0$ e use os itens (b) e (c) do lema 1.1.

3. Para $f(X) = X^2 + 2iX - 1$ temos que i é raiz mas $-i$ não é raiz.

4. Use o corolário 3.25 e o resultado do problema 2.

5. Se $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, com $a_n \neq 0$, segue de $f(\alpha) = 0$ que $\alpha^n = -\frac{a_{n-1}}{a_n} \cdot \alpha^{n-1} - \cdots - \frac{a_1}{a_n}\alpha - \frac{a_0}{a_n}$. Agora, argumente por indução para provar (3.9) para $m \geq n$. Para provar (3.9) para $m = -1$, escreva a igualdade $\alpha^{-1} f(\alpha) = 0$ em termos dos coeficientes de f; para o caso $m < 0$ geral, use novamente indução.

6. Use a desigualdade triangular para concluir que, se $|z| \geq 1$, então

$$|a_n||z|^n \leq |a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0| \leq nA|z|^{n-1}.$$

7. Se $z = \alpha + \beta i$ é uma raiz complexa de f tal que $\alpha > 2$, use a desigualdade triangular, no espírito da sugestão dada ao problema anterior, para concluir que $|a_n z^n + a_{n-1} z^{n-1}| < \frac{k|z|^{n-1}}{|z|-1}$; mostre, a partir daí, que $|z| < 1 + \frac{k}{|a_n z + a_{n-1}|}$ e, por fim, substitua $z = \alpha + i\beta$.

8. Para o caso de grau quatro, se $z \in \mathbb{C}$ é uma raiz, então $z \neq 0$ e $a\left(z^2 + \frac{1}{z^2}\right) + b\left(z + \frac{1}{z}\right) + c$; faça agora a mudança de variável $w = z + \frac{1}{z}$. Para o caso de grau seis, raciocine analogamente.

9. Use a condição do enunciado para obter a forma fatorada do polinômio $g(X) = (X+1)f(X) - X$.

10. Mostre inicialmente que, se a, b e c são tais raízes, então a hipótese de que a, b e c são positivos garante que a, b e c são os lados de um triângulo se, e somente se, $(a+b-c)(a+c-b)(b+c-a) > 0$; em seguida, substitua $a + b + c = -p$ no primeiro membro dessa desigualdade e use a forma fatorada $(X-a)(X-b)(X-c)$ do polinômio.

11. Assim como no exemplo 3.27, substitua X por 1 na forma fatorada de $X^{n-1} + X^{n-2} + \cdots + X + 1$. Em seguida, use um pouco de trigonometria para mostrar que, se $\omega = \mathrm{cis}\,\frac{2\pi}{n}$, então $|1 - \omega^k| = 2\mathrm{sen}\,\frac{k\pi}{n}$, para $1 \leq k \leq n$.

12. Use o resultado do problema anterior, juntamente com a relação $\mathrm{sen}\,(\pi - x) = \mathrm{sen}\,x$, para $x \in \mathbb{R}$.

13. Se $z \in \mathbb{C}$ for uma raiz de p, mostre que z^2 e $z - 1$ também o são. A partir daí, conclua sucessivamente que $|z| = 1$, $|z - 1| = 1$ e $z = \omega$ ou $z = \overline{\omega}$, onde $\omega = \mathrm{cis}\,\frac{2\pi}{3}$. Por fim, use o resultado do problema 2.

Seção 3.4

1. Use o resultado do corolário 3.32, nos moldes do exemplo 3.33, para mostrar que $8a^3 - 25a^2 - 180a + 608 = 0$. Em seguida, conclua que $a = 4$.

2. Escreva $f(X) = g(X)^2 h(X)$ e, em seguida, calcule f'.

3. Use o item (b) da proposição 3.29 para mostrar que $f'(z) = \sum_{j=1}^{n} \frac{f(z)}{z - z_j}$.

4. Use o item (b) da proposição 3.29 para mostrar quer

$$f'(z) = \sum_{j=1}^{n} \frac{f_j'(z)}{f_j(z)} f(z).$$

5. Pondo $f(X) = \prod_{k=1}^{n}\left(1 + \frac{1}{k}X^k\right)$, mostre que $f(1) = n + 1$. Em seguida, mostre que

$$f(X) = 1 + \sum_{\emptyset \neq S \subset I_n} \frac{1}{\pi(S)} X^{\sigma(S)}$$

e calcule $f'(1)$. Por fim, calcule $\frac{f'(1)}{f(1)}$ com o auxílio do problema anterior.

6. Basta mostrar que, se um semiplano qualquer do plano complexo contiver as raízes de f, então ele também conterá as raízes de f'. Por absurdo, suponha que exista uma reta r tal que um dos semiplanos que ela determina contém uma raiz w de f', enquanto o outro contém as raízes de f. Seja $u \in \mathbb{C}$ de módulo 1 e tal que o vetor $\mathbf{u}$ é perpendicular a r; se $f(X) = a(X - z_1)\ldots(X - z_n)$ e θ e θ_j são respectivamente os argumentos de u e de $z_j - w$, use o resultado do problema 3 para mostrar que

$$\mathrm{Re}\left(\sum_{j=1}^{n} |z_j - w|^{-1}\cos(\theta_j - \theta)\right) = 0.$$

Agora, observe que $(z_j - w)/u$ tem um argumento em $(-\frac{\pi}{2}, \frac{\pi}{2})$ e use a igualdade acima para chegar a uma contradição.

7. Se $f(X) = \sum_{k=0}^{n} c_k X^k$, com $c_k \in \mathbb{Z}$, então $f(X) = \sum_{k=0}^{n} c_k(a + X - a)^k$. Expanda a expressão do segundo membro em potências de $X - a$ e compare o resultado com (3.10), quando $z = a$.

8. Faça indução sobre $k \geq 1$. Para o passo de indução, se $m_k \in \mathbb{N}$ for tal que $f(m_k) \equiv 0 \pmod{p^k}$ e $f'(m_k) \not\equiv 0 \pmod{p}$, faça $m_{k+1} = m_k + xp^k$, com $x \in \mathbb{Z}$ a determinar. Em seguida, use a fórmula de Taylor (3.10), juntamente com o resultado do problema anterior, para mostrar que

$$f(m_{k+1}) \equiv f(m_k) + f'(m_k)xp^k \pmod{p^{k+1}};$$

a partir daí, mostre que é possível escolher x de forma que $f(m_{k+1}) \equiv 0 \pmod{p^{k+1}}$. Por fim, como $m_{k+1} \equiv m_k \pmod{p}$ e $f' \in \mathbb{Z}[X]$, temos $f'(m_{k+1}) \equiv f'(m_k) \not\equiv 0 \pmod{p}$.

Seção 4.1

1. Adapte, ao presente caso, a demonstração da proposição 4.1.

2. Para o item (a), adapte a ideia da solução do exemplo 4.3. Para o item (b), comece escrevendo

$$(X-Y)^5 + (Y-Z)^5 + (Z-X)^5 = (X-Y)(Y-Z)(Z-X)f(X,Y,Z),$$

com f de grau 2; em seguida, use a igualdade $-y^5 + (y - z)^5 + z^5 = -yz(y-z)f(0,y,z)$ para mostrar que $f(0,Y,Z) = 5(Y^2 - YZ + Z^2)$ e, analogamente, $f(X,0,Z) = 5(X^2 - XZ + Z^2)$ e $f(X,Y,0) = 5(X^2 - XY + Y^2)$. Por fim, mostre que

$$f(X,Y,Z) = 5(X^2 + Y^2 + Z^2 - XY - XZ - YZ).$$

3. Adapte a ideia da solução do exemplo 4.3 para concluir que

$$f(X,Y,Z) = (X+Y)(X+Z)(Y+Z)g(X,Y,Z),$$

com g de grau 2. Agora, use a igualdade $f(0,y,z) = yzg(0,y,z)$ para mostrar que $g(0,Y,Z) = Y^2 + YZ + Z^2$ e, analogamente, $g(X,0,Z) = X^2 + XZ + Z^2$ e $g(X,Y,0) = X^2 + XY + Y^2$. Por fim, mostre que

$$g(X,Y,Z) = X^2 + Y^2 + Z^2 + XY + XZ + YZ.$$

Seção 4.2

1. Use a simetria de f e g para mostrar que, fixada uma permutação σ de I_n, temos $h(x_1, \ldots, x_n) = h(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ para infinitos $x_1, \ldots, x_n \in K$. Você precisará utilizar o resultado do problema 1, página 90, bem como o resultado da proposição 4.1.

4. Fazendo $a^2 + b^2 + c^2 = k$, temos $a^3 + 3a^2 = 3k - 25$, de modo que a é raiz de $f(X) = X^3 + 3X^2 + (25 - 3k)$; analogamente, b e c são raízes de tal polinômio. Agora, use as relações de Girard para concluir que $a + b + c = -3$ e $ab + ac + bc = 0$, de sorte que $a^2 + b^2 + c^2 = 9$.

5. Sendo z_1, z_2, z_3 as raízes complexas do polinômio dado, o polinômio desejado é $f(X) = (X - z_1^3)(X - z_2^3)(X - z_3^3)$. Use as relações de Girard, juntamente com o resultado do exemplo 4.3, para calcular os coeficientes de f em termos dos complexos dados a, b e c. Por exemplo, sendo $g(X) = X^3 + aX^2 + bX + c$, temos $g(X) = (X - z_1)(X - z_2)(X - z_3)$ e, daí,

$$\begin{aligned} z_1^3 + z_2^3 + z_3^3 &= (z_1 + z_2 + z_3)^3 - 3(z_1 + z_2)(z_1 + z_3)(z_2 + z_3) \\ &= (-a)^3 - 3(-a - z_3)(-a - z_2)(-a - z_1) \\ &= -a^3 - 3g(-a) = -a^3 + 3ab - 3c. \end{aligned}$$

6. Para o item (a), use os resultados do problema 2, página 74 e do exemplo 4.7; para o item (b), use o resultado do problema anterior.

7. Adapte o argumento do exemplo 4.7.

8. Se $f(X) = (X - a)(X - b)(X - c)$, então $f(X) = X^3 - p$, onde $p = abc \neq 0$; argumente, agora, como na sugestão ao problema 5, página 75.

9. Aplique o resultado do exemplo 4.7 ao polinômio $g(X) = X^{100} + 2X^{99} + 3X^{98} + \cdots + a_{98}X^2 + a_{99}X + a_{100}$; em seguida, mostre que as raízes de g são os inversos das raízes de f.

10. Sendo $ax + by = c$ a equação de uma reta satisfazendo as condições do enunciado, substitua $y = -\frac{b}{a}x - \frac{c}{a}$ na equação que define o gráfico de f e, em seguida, use as relações de Girard para calcular o valor de $x_1 + x_2 + x_3 + x_4$.

11. Sendo $(x - a)^2 + (y - b)^2 = R^2$ a equação do círculo, substitua $y = \frac{1}{x}$ na mesma, utilizando em seguida as relações de Girard para calcular o produto das abscissas dos pontos de interseção.

12. Para o item (a), use o corolário 3.32. Para o item (b), use o fato de que $a^3 = a^2 + a + 1$, e analogamente para b e c; para o item (c), use (b) e as relações de Girard.

13. Para o item (a), use indução; para o item (b), observe inicialmente que

$$f(X) = X^n + s_1X^{n-1} + s_2X^{n-2} + \cdots + s_{n-1}X + s_n.$$

14. Faça indução sobre $n > 1$ para concluir que $x_1 = x_2 = \cdots = x_n = 1$. Para o passo de indução, se

$$\begin{aligned} f(X) &= (X - x_1)(X - x_2)\cdots(X - x_n) \\ &= X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \end{aligned}$$

conclua que

$$\begin{aligned} 0 &= f(x_1) + f(x_2) + \cdots + f(x_n) \\ &= n + a_{n-1}n + \cdots + a_1n + a_0n = nf(1). \end{aligned}$$

15. Conclua inicialmente que as raízes de f são negativas; em seguida, use as relações de Girard e a desigualdade entre as médias aritmética e geométrica para deduzir que $a_k \geq \binom{n}{k}$, para $1 \leq k \leq n - 1$.

16. Sendo $x_1, \ldots, x_n$ as raízes de f, use as relações de Girard para concluir que $\sum_{i=1}^n x_i^2 = 3$ e $\prod_{i=1}^n x_i^2 = 1$; então, aplique a desigualdade entre as médias aritmética e geométrica para concluir que $n \leq 3$. Por fim, considere separadamente cada um dos casos aos quais o problema ficou reduzido.

Seção 4.3

1. Para $1 \leq k \leq n$ use o teorema de Newton e as relações de Girard; para $k \geq n + 1$, use o item (a) da proposição 4.17.

2. Use o item (b) da proposição 4.17 para provar, por indução sobre i, que as $i-$ésimas somas simétricas elementares de $a_1, \ldots, a_n$ e $b_1, \ldots, b_n$ coincidem, para $1 \leq i \leq n$; em seguida, compare os coeficientes dos polinômios $\prod_{j=1}^n(X - a_j)$ e $\prod_{j=1}^n(X - b_j)$.

3. Use o item (b) da proposição 4.17 para provar, por indução sobre j, que $s_j = \binom{n}{j}$, para $1 \leq j \leq k$.

4. Para o item (a), fatore $X^m - z^m$ sobre $\mathbb{C}$ e use o resultado para fatorar g sobre $\mathbb{C}$.

5. Para o item (a), se $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ é um polinômio de coeficientes inteiros e tal que todas as suas raízes complexas têm módulo 1, use as relações de Girard para mostrar que $|a_{n-k}| \leq \binom{n}{k}$, para $0 < k \leq n$. Para o item (b), sejam $\alpha_1, \ldots, \alpha_n$ as raízes de f. Mostre, com o auxílio do teorema de Newton, que o polinômio $f_k(X) = (X - \alpha_1^{2^k}) \ldots (X - \alpha_n^{2^k})$ tem coeficientes inteiros, para todo $k \geq 1$. Em seguida, use o item (a) para garantir a existência de naturais $k < l$ tais que $f_k = f_l$. Por fim, use tal igualdade para mostrar que α_i é uma raiz da unidade, para $1 \leq i \leq n$.

Seção 5.1

1. Para cada raiz complexa não real $z = a + bi$ de f, escreva o fator $(X - z)(X - \overline{z})$ de f como na prova do lema 5.1. Em seguida, ponha f na forma fatorada e mostre que $|f(m)| \neq 0, 1$.

2. Se $\alpha < a < \beta$ são as raízes de f mais próximas de a, aplique o teorema de Bolzano a intervalos do tipo (a, b) ou (b, a) contidos no intervalo (α, β).

3. Por contradição, suponha $f'(a) > 0$ (o outro caso é análogo) e aplique o item (a) do corolário 5.7, juntamente com o resultado do problema anterior.

4. Aplique o teorema de Bolzano, o corolário 5.7 e o resultado do problema anterior, observando que $f'(x) = 0 \Leftrightarrow x = 0$ ou $x = \frac{8}{5}$ e $f(-1), f(\frac{8}{5}) < 0 < f(0)$.

5. Tome n_0 maior que as maiores raízes reais de f e de f'. Use o teorema de Bolzano, juntamente com o fato de que $f(x) > 0$ para x suficientemente grande (conforme estimativa análoga à que precede (3.7)) para mostrar que $f(x) > 0$ para $x > n_0$. Em seguida, use o corolário 5.7 para mostrar que $f(u) > f(v)$ para $u > v > n_0$.

6. Tome, de acordo com o problema anterior, $n_0 \in \mathbb{N}$ tal que $u > v > n_0 \Rightarrow f(u) > f(v) > 0$. Em seguida, se $m > n_0$ é um inteiro tal que $f(m) = p$, um número primo, mostre que $f(m + p^2)$ é composto.

7. Inicialmente, mostre que a condição do enunciado equivale a $x^{11} - x = y^{11} - y$. Em seguida, prove que, para qualquer $c \in \mathbb{R}$, o polinômio $f(x) = X^{11} - X - c$ tem no máximo três raízes reais distintas; para tanto, você precisará utilizar os resultados do corolário 5.7 e do problema 3, de maneira análoga àquela delineada na sugestão ao problema 4.

8. Como $\lambda \neq 0$, mostre que λ é raiz do polinômio do enunciado se, e só se, $f(\lambda) = 1$, onde $f(X) = (X - a_1)(X - a_2)(X - a_3)(X - a_4)$. Agora, mostre que f é decrescente em $(-\infty, a_1)$, de sorte que $f(0) = 1$ garante que $\lambda \geq a_1$. Por fim, note que, se $a_1 \leq \lambda \leq a_2$, então $f(\lambda) \leq 0$.

9. Sejam $f(X) = aX^4 + bX^3 + cX^2 + dX + e$ e $t > 1$ tal que t^2 é uma raiz real de $aX^2 + (c - b)X + (e - d)$. Mostre que $f(t)f(-t) = (bt^2 + d)(1 - t^2) < 0$ e, em seguida, use o teorema de Bolzano.

10. Faça
$$f(X) = \sum_{i=1}^{n} a_i X^i, \quad g(X) = \sum_{i,j=1}^{n} \frac{a_i a_j}{i + j} X^{i+j}$$
e conclua que $xg'(x) = f(x)^2 \geq 0$, para todo $x \geq 0$. Em seguida, use o corolário 5.7 para concluir que $g(1) \geq g(0) = 0$, com igualdade se, e só se, g for constante.

11. Comece mostrando que f tem três raízes reais distintas $\alpha < \beta < \gamma$, tais que $-2 < \alpha < -1$, $0 < \beta < 1$ e $1 < \gamma < 2$. Em seguida, observe

que $f(f(x)) = 0$ se, e só se, $f(x) = \alpha$, β ou γ. Por fim, examine as quantidades de raízes reais distintas de cada um dos polinômios $f(X) - \alpha$, $f(X) - \beta$ e $f(X) - \gamma$.

12. Seja $g(x) = f(x) + f'(x) + f''(x) + \cdots + f^{(n)}(x)$ e suponha, por contradição, que g assume valores negativos. Então, $f \neq 0$ e a condição $f(x) \geq 0$ para $x \in \mathbb{R}$ garante que n é par e o coeficiente líder de f é positivo. Portanto, $\lim_{|x| \to +\infty} f(x) = +\infty$, e o teorema de Weierstrass (o teorema 4.31 de [12]) garante a existência de $x_0 \in \mathbb{R}$ tal que g assume seu valor mínimo em x_0, valor este negativo. Segue do problema 3 que $g'(x_0) = 0$. Mas, como

$$g'(x_0) = f'(x_0) + f''(x_0) + \cdots + f^{(n)}(x_0),$$

temos que

$$0 > g(x_0) = f(x_0) + g'(x_0) = f(x_0) \geq 0,$$

o que é uma contradição.

13. Mostre inicialmente que B pode jogar de forma tal que, quando faltarem ser escolhidos exatamente três coeficientes, ao menos dois deles sejam coeficientes de termos X^r, com r ímpar. Em seguida, após A jogar, teremos $f(X) = g(X) + aX^k + bX^l$, sendo g um polinômio completamente determinado, $1 \leq k, l \leq 2n - 1$ inteiros distintos e a e b coeficientes a escolher, tais que pelo menos l é ímpar. Por fim, como $f(2) = g(2) + 2^k a + 2^l b$ e $f(-1) = g(-1) + (-1)^k a - b$, teremos $f(2) + 2^l f(-1) = g(2) + 2^l g(-1) + (2^k + (-1)^k 2^l)a$, de forma que B pode jogar escolhendo $a = -\frac{g(2)+2^l g(-1)}{2^k+(-1)^k 2^l}$. Conclua que, após tal jogada de B, teremos $f(2) + 2^l f(-1) = 0$, de sorte que, pelo TVI, f terá pelo menos uma raiz real, independentemente da última jogada de A.

14. Sem perda de generalidade, suponha que o coeficiente líder do polinômio f, originalmente escrito na lousa, é positivo, e sejam α a menor e β a maior raiz real de f. Se $\alpha < \beta$, mostre que $f'(\alpha) > 0$ ou $f'(\beta) > 0$; se $f'(\beta) > 0$ (o caso $f'(\alpha) > 0$ é análogo), conclua que o próximo polinômio escrito na lousa ou não tem raiz no intervalo $[\beta, +\infty)$ ou tem uma raiz em $(\beta, +\infty)$. Se $\alpha = \beta$, de sorte que $f(X) = (X - \alpha)^3$, mostre que $f \pm f'$ se enquadra no primeiro caso.

15. Se $b_i = -a_i$ para $1 \leq i \leq n$, mostre que a condição $f(x) \geq 1$ equivale a $\frac{p(x)}{q(x)} \leq 0$, onde $q(X) = \prod_{i=1}^n (X - b_i)$ e

$$p(X) = \prod_{i=1}^n (X - b_i) + \sum_{i=1}^n \left(b_i \prod_{j \neq i} (X - b_j) \right).$$

Mostre que p tem uma raiz $x_1 \in (b_1, +\infty)$; em seguida, use o teorema de Bolzano para mostrar que p também possui uma raiz x_i em cada um dos intervalos (b_i, b_{i-1}), para $2 \leq i \leq n$. Analisando separadamente os casos n par e n ímpar, mostre que a soma dos comprimentos dos intervalos-solução da inequação $\frac{p(x)}{q(x)} \leq 0$ é $|\sum_{i=1}^n x_i - \sum_{i=1}^n b_i|$. Por fim, use as relações de Girard para mostrar que $\sum_{i=1}^n x_i = 0$.

Seção 5.3

1. Se f denota o polinômio do enunciado e $g(X) = (X - 1)f(X)$, então $g(X) = X^{n+1} - 2X^n + 1$. Conclua, a partir da regra de Descartes, que g tem no máximo duas raízes reais positivas e, daí, que f tem uma única raiz positiva, a qual deve ser a_n (alternativamente, apele para o exemplo 5.17). Para concluir, é suficiente, pelo teorema de Bolzano, mostrar que $f\left(2 - \frac{1}{2^{n-1}}\right)$ e $f\left(2 - \frac{1}{2^n}\right)$ têm sinais contrários. Por fim, use o fato de que $1 < 2 - \frac{1}{2^{n-1}} < 2 - \frac{1}{2^n}$ para mostrar que é suficiente provar que $g\left(2 - \frac{1}{2^{n-1}}\right)$ e $g\left(2 - \frac{1}{2^n}\right)$ têm sinais contrários.

2. Se $f(X) = aX^3 + bX^2 + cX + d$, queremos calcular o número de raízes reais de $g = 2ff'' - (f')^2$. Suponha, sem perda de generalidade, que $a = 1$; ademais, se $\alpha < \beta < \gamma$ são as raízes de f, mostre que, trocando $g(X)$ por $h(X) = g(X + \beta)$, podemos supor, sem perda

de generalidade, que $\beta = 0$ e, daí, que $c < 0$ e $d = 0$. Sob tais simplificações, um cálculo imediato fornece $g(X) = 3X^4 + 4bX^3 + 6cX^2 - c^2$. Basta, agora, usar a regra de Descartes para concluir que g tem exatamente uma raiz positiva e exatamente uma raiz negativa.

Seção 6.1

1. Para o item (i), use o fato de que $\partial f_j = j$ para concluir que $a_n = b_n$; em seguida, argumente por indução. Para (ii), tome $n = \partial f$ e argumente por indução sobre n; para o passo de indução, comece escolhendo a_n igual ao coeficiente líder de f.

2. Para $k = 0$ e $k = 1$, o resultado é trivial. Para $k \geq 2$, mostre que $\binom{X}{k}(x) = 0$ se $0 \leq x \leq k-1$, $\binom{X}{k}(x) = \binom{x}{k}$ se $x \geq k$ e $\binom{X}{k}(x) = (-1)^k\binom{-x-1+k}{k}$, se $x < 0$.

3. Aplique o teorema de interpolação de Lagrange.

4. Aplique o teorema de interpolação de Lagrange.

6. Adapte, ao presente caso, a demonstração da proposição 6.6.

7. Faça $\omega = \text{cis}\,\frac{2\pi}{n}$; em seguida, para $1 \leq k \leq n-1$ substitua $x = \omega^k$ nas funções polinomiais correspondentes a p e aos p_j's e use o resultado da proposição 6.6.

8. Para cada um dos primos p do conjunto $A = \{3, 5, 7, 11, 13, 17\}$, seja α_p o valor comum das somas $a_k + a_{k+p} + a_{k+2p} + \cdots$ quando k varia de 1 a p, e $\omega_p = \text{cis}\,\frac{2\pi}{p}$. Se $f(X) = a_{50}X^{50} + \cdots + a_2X^2 + a_1X$, aplique a versão geral da fórmula de multiseção (dada pelo problema 5) para $r = 0, 1, \ldots, p-1$, a fim de obter um sistema linear de equações do tipo (6.2) nas p incógnitas $f(\omega_p^j)$, $0 \leq j \leq p-1$. Conclua, com o auxílio da proposição 6.6, que a solução de tal sistema é $f(1) = p\alpha_p$ e $f(\omega_p) = \cdots = f(\omega_p^{p-1}) = 0$, obtendo, assim, $p-1$ raízes distintas e não nulas para f. Por fim, notando que $\sum_{p\in A}(p-1) = 50$ e que 0 também é raiz de f, conclua que $f = 0$.

Seção 6.2

1. Façamos indução sobre $k \geq 1$, sendo o caso $k = 1$ imediato. Suponha, por hipótese de indução, que a fórmula valha para um certo $k \in \mathbb{N}$. Para $k+1$, temos:

$$\begin{aligned}
f(x+(k+1)h) &= f(x+kh) + (\Delta_h^1 f)(x+kh) \\
&= f(x+kh) + \sum_{j=0}^{k}\binom{k}{j}(\Delta_h^{k-j}(\Delta_h^1 f))(x) \\
&= \sum_{j=0}^{k}\binom{k}{j}(\Delta_h^{k-j} f)(x) + \sum_{j=0}^{k}\binom{k}{j}(\Delta_h^{k+1-j} f)(x) \\
&= \sum_{j=0}^{k}\binom{k}{j}(\Delta_h^{k-j} f)(x) + (\Delta_h^{k+1} f)(x) \\
&\quad + \sum_{j=1}^{k}\binom{k}{j}(\Delta_h^{k-(j-1)} f)(x).
\end{aligned}$$

Agora, executando uma troca de índices na última soma acima e utilizando a relação de Stifel, obtemos $f(x+(k+1)h)$ sucessivamente igual a

$$\begin{aligned}
&\sum_{j=0}^{k}\binom{k}{j}(\Delta_h^{k-j} f)(x) + (\Delta_h^{k+1} f)(x) + \sum_{j=0}^{k-1}\binom{k}{j+1}(\Delta^{k-j} f)(x) \\
&= (\Delta_h^{k+1} f)(x) + (\Delta_h^0 f)(x) \\
&\quad + \sum_{j=0}^{k-1}\left(\binom{k}{j} + \binom{k}{j+1}\right)(\Delta_h^{(k+1)-(j+1)} f)(x) \\
&= \sum_{j=0}^{k+1}\binom{k+1}{j}(\Delta_h^{k+1-j} f)(x).
\end{aligned}$$

2. Adapte, ao presente caso, as soluções dos exemplos 6.15 e 6.15.

3. Como $\partial f = n$, a proposição 6.14 garante que $\Delta^{n+1} f = 0$, onde escrevemos Δ^k para denotar Δ_1^k. Portanto, segue do item (e) da

proposição 6.13 que

$$\begin{aligned}
0 = (\Delta^{n+1}f)(0) &= \sum_{j=0}^{n+1}(-1)^j\binom{n+1}{j}f(n+1-j) \\
&= \sum_{j=1}^{n+1}(-1)^j\binom{n+1}{j}\cdot\frac{1}{\binom{n+1}{n+1-j}} + f(n+1) \\
&= \sum_{j=1}^{n+1}(-1)^j + f(n+1),
\end{aligned}$$

de maneira que

$$f(n+1) = -\sum_{j=1}^{n+1}(-1)^j = \begin{cases} 0, & \text{se } n \equiv 1 \pmod 2 \\ 1, & \text{se } n \equiv 0 \pmod 2 \end{cases}.$$

4. Use o item (e) da proposição 6.13 para obter a igualdade

$$0 = (\Delta_1^{991}f)(992) = \sum_{j=0}^{991}(-1)^j\binom{991}{j}f(1983-j).$$

Em seguida, utilize o lema 2.12 de [13], juntamente com o resultado do problema 18 da seção 6.2 de [10].

5. As condições do enunciado garantem que $(\Delta_1^k f)(0) > 0$ para $0 \le k \le 3$ e $(\Delta_1^4 f)(n) > 0$ para todo $n \in \mathbb{N}$. Mostre agora que, para todo $m \in \mathbb{N}$, temos

$$(\Delta_1^{m-1}f)(n) = \sum_{k=0}^{n-1}(\Delta_1^m f)(k) + (\Delta_1^{m-1}f)(0)$$

e, por fim, use a fórmula acima para mostrar sucessivamente que $(\Delta_1^3 f)(n) > 0$, $(\Delta_1^2 f)(n) > 0$, $(\Delta_1 f)(n) > 0$ e $f(n) = (\Delta_1^0 f)(n) > 0$, para todo $n \in \mathbb{N}$.

Seção 7.1

2. Inicialmente, mostre que $p_1^{\gamma_1}\ldots p_k^{\gamma_k}$ divide ambos f e g em $\mathbb{Q}[X]$. Para o que falta, comece mostrando que, se $h \in \mathbb{Q}[X]$ é mônico e tal que $h \mid f$ em $\mathbb{Q}[X]$, então $h = p_1^{\delta_1}\ldots p_k^{\delta_k}q_1^{\delta_1'}\ldots q_l^{\delta_l'}$, com $0 \le \delta_i \le \alpha_i$, para $1 \le i \le k$, e $0 \le \delta_i' \le \alpha_i'$, para $1 \le i \le l$.

3. Argumente por contraposição.

5. Comece utilizando o corolário 3.25, juntamente com o problema 2, página 74, nos moldes do item (b) do exemplo 7.7.

6. Para o item (a), faça indução sobre k, utilizando o corolário 7.4 para mostrar que existem $\tilde{f}_1, f_k \in \mathbb{K}[X]$ tais que $\frac{f}{g} = \frac{\tilde{f}_1}{g_1^{\alpha_1}\cdots g_{k-1}^{\alpha_{k-1}}} + \frac{f_k}{g_k^{\alpha_k}}$, com $\tilde{f}_1 = 0$ ou $\partial\tilde{f}_1 < \partial(g_1^{\alpha_1}\ldots g_{k-1}^{\alpha_{k-1}})$ e $f_k = 0$ ou $\partial f_k < \partial(g_k^{\alpha_k})$. Para o item (b), comece dividindo f por g^k, obtendo $f = g^k q + r$, com $r = 0$ ou $0 \le \partial r < \partial(g^k)$; em seguida, divida r por g^{k-1} e proceda indutivamente.

Seção 7.2

2. Como f é redutível sobre $\mathbb{Q}$, existem $g_1, h_1 \in \mathbb{Q}[X]$ mônicos, não constantes e tais que $f = g_1h_1$. Tome $a, b, c, d \in \mathbb{Z}\setminus\{0\}$ tais que $\text{mdc}(a,b) = \text{mdc}(c,d) = 1$ e $g_1 = \frac{a}{b}g$, $h_1 = \frac{c}{d}g$, com $g, h \in \mathbb{Z}[X]$ mônicos e não constantes. Como $bdf(X) = acg(X)h(X)$, tome conteúdos e use o lema de Gauss para concluir que $bd = ac$.

Seção 7.3

2. Note primeiro que

$$f(a) = 0 \Rightarrow \overline{f(a)} = \overline{0} \Rightarrow \overline{f}(\overline{a}) = \overline{0}.$$

A segunda afirmação é imediata.

5. Se $a \in \mathbb{Q}$ for uma possível raiz racional de f, o critério de pesquisa de raízes racionais garante que $a \in \mathbb{Z}$ e $a \mid 84$, mas ainda fornece muitas possibilidades para a; a fim de eliminar várias delas, projete f em $\mathbb{Z}_3[X]$ e em $\mathbb{Z}_5[X]$ para concluir, com o auxílio do problema 2, que $a \equiv 0 \pmod 3$ e $a \equiv 4 \pmod 5$, de sorte que $a = -6, -21$ ou 84.

6. Faça indução sobre ∂f; no passo de indução você terá de usar que $p \mid \binom{p}{k}$, para $1 \leq k \leq p-1$.

7. Suponha que fg não é primitivo e fixe um primo p que divide todos os seus coeficientes. A partir da igualdade $\overline{f}\overline{g} = \overline{fg} = \overline{0}$ em $\mathbb{Z}_p[X]$, conclua que $\overline{f} = \overline{0}$ ou $\overline{g} = \overline{0}$.

8. Use o resultado da proposição 7.19, juntamente com as relações de Girard.

9. Mostre que, módulo 17, temos

$$X^3 - \overline{3}X^2 + \overline{1} = (X - \overline{4})(X - \overline{5})(X + \overline{6}).$$

Em seguida, ponha $s_k = a^k + b^k + c^k$, $t_k = 4^k + 5^k + (-6)^k$ e conclua (com o auxílio dos métodos da seção 4.2) que

$$\begin{cases} s_{k+3} - 3s_{k+2} + s_k = 0 \\ s_1 = 3, s_2 = 0, s_3 = -1 \end{cases} \text{ e } \begin{cases} t_{k+3} - 3t_{k+2} + t_k = 0 \\ t_1 = 3, t_2 = 0, t_3 = -1 \end{cases}.$$

A partir daí, mostre que $s_n \in \mathbb{Z}$, para todo $n \in \mathbb{N}$, e $s_n \equiv t_n \pmod{17}$.

Seção 7.4

1. Inicialmente, use o critério de pesquisa de raízes racionais para mostrar que o polinômio dado não tem raízes inteiras. Em seguida, analise a possibilidade $X^4 - X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d)$, com $a, b, c, d \in \mathbb{Z}$.

2. Pelo lema de Gauss, basta mostrarmos que f não pode ser escrito como o produto de dois polinômios não constantes de coeficientes inteiros. Para tanto, observe inicialmente que, pelo critério de pesquisa de raízes racionais, f não possui raízes racionais; portanto, se f pudesse ser escrito como o produto de dois polinômios não constantes de coeficientes inteiros, deveríamos ter

$$f(X) = (X^2 + aX + b)(X^3 + cX^2 + dX + e),$$

para certos $a, b, c, d, e \in \mathbb{Z}$. Desenvolvendo o produto do segundo membro acima e comparando coeficientes de mesmo grau, concluímos que deveria ser $be = 2$, de forma que $(b, e) = (1, 2)$, $(-1, -2)$, $(2, 1)$ ou $(-2, -1)$. Mas, verifica-se facilmente que nenhuma dessas possibilidades é compatível com as demais equações obtidas da comparação dos coeficientes.

3. Escreva $f(X^n) = g(X)h(X)$, com $g, h \in \mathbb{R}[X] \setminus \mathbb{R}$ como prescrito pelo enunciado e $n > 1$ (o caso $n = 1$ é trivial). Se $g(X) = b_kX^k + b_{k+1}X^{k+1} + \cdots$ e $h(X) = c_lX^l + c_{l+1}X^{l+1} + \cdots$, com $b_k, c_l \neq 0$, então, trocando g e h respectivamente por $g(X) = b_k + b_{k+1}X + \cdots$ e $h(X) = c_lX^{k+l} + c_{l+1}X^{k+l+1} + \cdots$, podemos supor que $g(0) \neq 0$. Sejam, pois, $g(X) = b_0 + b_1X + \cdots$ e $h(X) = c_lX^l + c_{l+1}X^{l+1} + \cdots$, com $b_0, c_l \neq 0$. Use o fato de que $f(X^n) = g(X)h(X)$ para mostrar que $n \mid l$. Em seguida, cancele os termos de grau mínimo em ambos os membros da igualdade $f(X^n) = g(X)h(X)$ e argumente por indução sobre ∂f para mostrar que $g(X) = g_1(X^n)$ e $h(X) = h_1(X^n)$, para certos $g_1, h_1 \in \mathbb{R}[X] \setminus \mathbb{R}$ como prescrito pelo enunciado.

4. Pelo lema de Gauss, é suficiente examinar quando $f = gh$, com g e h polinômios mônicos, não constantes e de coeficientes inteiros. Adaptando a ideia da prova do exemplo 7.32, temos $1 = f(0) = g(0)h(0)$, de sorte que $g(0) = h(0) = \pm 1$; portanto, $a_1, a_2, \ldots, a_n$ são raízes duas a duas distintas do polinômio $g - h$. Se $g - h \neq 0$, então, $\partial(g - h) \leq \max\{\partial g, \partial h\} < \partial f = n$, de sorte que $g - h$ teria menos de n raízes distintas. Logo, $g - h = 0$ e, daí, $f = g^2$ ou, ainda,

$$g(X)^2 - 1 = (X - a_1) \ldots (X - a_n).$$

Em particular, devemos ter $n = 2k$, para algum $k \in \mathbb{N}$. Suponha, sem perda de generalidade, que

$$g(X)-1 = (X-a_1)\dots(X-a_k) \text{ e } g(X)+1 = (X-a_{k+1})\dots(X-a_{2k}),$$

com $a_1 < a_2 < \cdots < a_k$ e $a_{k+1} < a_{k+2} < \cdots < a_{2k}$. Então,

$$2 = (X-a_{k+1})\dots(X-a_{2k}) - (X-a_1)\dots(X-a_k)$$

e, avaliando a igualdade acima respectivamente em $a_1, a_2, \dots, a_k$, obtemos

$$(a_i - a_{k+1})\dots(a_i - a_{2k}) = 2,$$

para $1 \leq i \leq k$. A partir daí, conclua que, se $k \geq 3$, então ao menos dois dos números $a_{k+1}, a_{k+2}, \dots, a_{2k}$ seriam iguais, o que não é o caso. Por fim, analise separadamente os casos $k = 1$ e $k = 2$ para obter os polinômios do enunciado.

5. Use o critério de Eisenstein, em conjunção com o resultado do item (a) do problema 8, página 178.

6. Use o teorema 7.27, em conjunção com o critério de pesquisa de raízes racionais (proposição 3.16).

7. Suponha $f = gh$, com $g, h \in \mathbb{Z}[X] \setminus \mathbb{Z}$, e examine a igualdade $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$ em $\mathbb{Z}_p[X]$.

8. Pelo lema de Gauss, basta mostrar que f é irredutível em $\mathbb{Z}[X]$. Por contradição, suponha que fosse $f = gh$, com g e h não constantes e de coeficientes inteiros e (sem perda de generalidade, uma vez que $f(0) = p$) $g(0) = \pm 1$. Use as relações de Girard para concluir que g, e então f, tem uma raiz complexa z de módulo menor ou igual a 1. Por fim, substitua a expressão de f na igualdade $f(z) = 0$ e use as hipóteses sobre os coeficientes de f para chegar a uma contradição.

9. Sejam $z_1, \dots, z_n$ as raízes complexas de f. Se $|z_j| \leq 1$, para algum

$1 \leq j \leq n$, então

$$\begin{aligned} |a_0| &= |a_1 z_j + \cdots + a_n z_j^n| \\ &\leq |a_1||z_j| + \cdots + |a_n||z_j|^n \\ &\leq |a_1| + \cdots + |a_n|, \end{aligned}$$

o que é um absurdo. Logo, $|z_j| > 1$, para $1 \leq j \leq n$. Suponha, agora, que $f = gh$, com $g, h \in \mathbb{Z}[X]\backslash\mathbb{Z}$, digamos $g(X) = b_0 + b_1 X + \cdots + b_r X^r$ e $h(X) = c_0 + c_1 X + \cdots + c_s X^s$. Reenumerando os z_j's, se necessário, podemos supor que as raízes de g são $z_1, \dots, z_r$. Então, segue das relações de Girard que

$$|b_0| = |b_r||z_1|\dots|z_r| > |b_r| \quad \text{e} \quad |c_0| = |c_s||z_{r+1}|\dots|z_n| > |c_s|.$$

Portanto, $|b_0| \geq |b_r| + 1$ e $|c_0| \leq |c_s| + 1$, de sorte que

$$\begin{aligned} |a_0| &= |b_0||c_0| \geq (|b_r| + 1)(|c_s| + 1) \\ &= |b_r||c_s| + |b_r| + |c_s| + 1 \\ &\geq |b_r||c_s| + 2\sqrt{|b_r||c_s|} + 1 \\ &= (\sqrt{|b_r||c_s|} + 1)^2 \\ &= (\sqrt{|a_n|} + 1)^2. \end{aligned}$$

Assim, $\sqrt{|a_0|} \geq \sqrt{|a_n|} + 1$, o que é um absurdo.

10. Para cada $1 \leq i \leq k$, escolha $a_i \in A_i$; em seguida, escolha um primo p tal que $p > a_1, \dots, a_k$. Se $A = \{pq;\ q \in \mathbb{N} \text{ e } p \nmid q\}$, mostre que existe $1 \leq j \leq k$ tal que $A \cap A_j$ é infinito. Por fim, aplique o critério de Eisenstein para mostrar que todo polinômio f de grau m, com coeficiente líder a_j e demais coeficientes em $A \cap A_j$ satisfaz a condição (c).

11. Para o item (a), use um argumento àquele da prova do lema 5.1. Para o item (b), suponha que $f = gh$, com $g, h \in \mathbb{Z}[X] \setminus \mathbb{Z}$. Então, segue de (a) que todos os coeficientes de $g_1(X) = g\left(X + m - \frac{1}{2}\right)$ têm um mesmo sinal. Portanto, $g_2(X) := g_1(-X)$ tem coeficientes

não nulos e de sinais alternados, de sorte que $|g_2(x)| < |g_1(x)|$ para todo $x > 0$ e, daí, $g\left(-x+m-\frac{1}{2}\right) < g\left(x+m-\frac{1}{2}\right)$, para todo $x > 0$; em particular, $|g(m-1)| < |g(m)|$. Conclua que $|g(m)| \geq 2$ e, analogamente, $|h(m)| \geq 2$. Por fim, use o fato de que $f(m)$ é primo para chegar a uma contradição.

12. Combine o teorema de Pólya-Szegö, dado pelo problema anterior, com o resultado do problema 7, página 75.

Seção 8.1

1. Se $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tem α por raiz, examine o polinômio

$$g(X) = \frac{a_n}{r^n}X^n + \frac{a_n}{r^{n-1}}X^{n-1} + \cdots + \frac{a_1}{r}X + a_0 \in \mathbb{Q}[X] \setminus \mathbb{Q}.$$

2. Pela primeira fórmula de de Moivre, temos $(\cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n})^n = 1$. Em seguida, desenvolva o binômio e utilize a relação fundamental da trigonometria para obter um polinômio não nulo, de coeficientes racionais e tendo $\cos\frac{2\pi}{n}$ por raiz.

3. Use o critério de Eisenstein 7.28.

4. Use primeiro o teorema de Gauss 7.15 para mostrar que existe $g \in \mathbb{Z}[X] \setminus \mathbb{Z}$, irredutível sobre $\mathbb{Z}$ e tal que $g(\alpha) = 0$. Conclua, com o auxílio do lema de Gauss 7.14 que g também é irredutível sobre $\mathbb{Q}$ e, daí, que $g = p_\alpha$.

5. Para o item (i), aplique duas vezes a observação 8.10, juntamente com o fato de que $p_{\sqrt{a}}(X) = X - \sqrt{a}$ ou $X^2 - a$, conforme $\sqrt{a} \in \mathbb{N}$ ou $\sqrt{a} \notin \mathbb{N}$ (e analogamente para $p_{\sqrt{b}}$ e $p_{\sqrt{c}}$). Para o item (ii), use (i) e o critério de pesquisa de raízes racionais.

6. Pelo problema 2, página 185, f é irredutível sobre $\mathbb{Q}$. Suponha, agora, que existam a e b inteiros primos entre si e $n > 1$ natural tais que $f(\alpha) = 0$, onde $\alpha = \sqrt[n]{|\frac{a}{b}|}$. Seja

$$g(X) = bX^n - a = b(X-\alpha)(X-\alpha\omega)\ldots(X-\alpha\omega^{n-1}),$$

onde $\omega = \mathrm{cis}\,\frac{2\pi}{n}$. Pelo corolário 8.4, temos que $f = p_\alpha$; portanto, o item (b) da proposição 8.3 garante que f divide g em $\mathbb{Q}[X]$ e, daí, em $\mathbb{Z}[X]$ (uma vez que $f \in \mathbb{Z}[X]$ e f é mônico). Portanto, segue do problema 2, página 74, que existem $1 \leq k < l \leq n-1$ tais que

$$f(X) = (X-\alpha)(X-\alpha\omega^k)(X-\alpha\overline{\omega}^k)(X-\alpha\omega^l)(X-\alpha\overline{\omega}^l).$$

Examinando o termo independente de f, segue que $-\alpha^5 = 2$ e, daí, $\alpha = -\sqrt[5]{2}$. Mas, como $h(X) = X^5 + 2$ é irredutível (pelo critério de Eisenstein) e $h(\alpha) = 0$, deveríamos ter $f = h$, o que é um absurdo.

7. Se $\alpha = \alpha_1, \ldots, \alpha_m$ são as raízes de p_α e $\beta = \beta_1, \ldots, \beta_n$ são as raízes de p_β, o candidato natural a analisar é

$$h(X) = \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (X - \alpha_i\beta_j) = (\alpha_1\ldots\alpha_m)^n \prod_{i=1}^{m} p_\beta\left(\frac{1}{\alpha_i}X\right).$$

Agora, observe que $\alpha_1\ldots\alpha_m = \pm p_\alpha(0) \in \mathbb{Q}$.

Seção 8.2

1. Use o item (a) da proposição 8.14 para $n = p^{k-1}$ e $n = p^k$.

2. Uma raiz típica de Φ_{2n} é $\omega = \mathrm{cis}\,\frac{2k\pi}{2n}$, tal que $1 \leq k \leq 2n$ e $\mathrm{mdc}\,(k, 2n) = 1$. Use, agora, o fato de que $-\omega$ também é dessa forma para concluir que $-\omega$ também é raiz de Φ_{2n}. Conclua, pois, que $\Phi_{2n}(X)$ é o produto de fatores do tipo $(X-\omega)(X+\omega)$.

3. Se Φ_m e Φ_n tivessem um fator não constante comum em $\mathbb{C}[X]$, então eles seriam idênticos, como polinômios minimais de uma qualquer de suas raízes comuns. Sendo $\Phi_m = \Phi_n = f$, seguiria do item (a) da proposição 8.14 que f^2 dividiria $X^{mn} - 1$, o que é um absurdo.

4. Primeiramente, veja que, com n e d como no enunciado, temos $\varphi(n) = \varphi(d) \cdot \frac{n}{d}$, de forma que $\partial\Phi_n = \partial f$, onde $f(X) = \Phi_d(X^{n/d})$. Agora, se $\omega = \text{cis}\,\frac{2k\pi}{n}$, com $1 \leq k \leq d$ e $\text{mdc}\,(k,d) = 1$, e $\eta \in \mathbb{C}$ é uma raiz $\frac{n}{d}$−ésima de ω, mostre que η é uma raiz primitiva n−ésima da unidade. Conclua, por fim, que Φ_n e f têm as mesmas raízes.

5. Pelo teorema de Dirichlet, escolha $d \in \mathbb{N}$ tal que $1 + kd = p$, um número primo. Em seguida, considere a PA $\frac{1}{(p-1)!}, \frac{1+d}{(p-1)!}, \ldots, \frac{1+(k-1)d}{(p-1)!}$.

6. A versão geral do teorema de Dirichlet garante que a PA $(n+2, 2n+2, 3n+2, \ldots)$ contém infinitos primos. Sendo $p = kn + 2 > a$ um qualquer deles e g uma raiz primitiva módulo p, segue do fato de $\{g, g^2, \ldots, g^{p-1}\}$ ser um SCR módulo p a existência de um inteiro $1 \leq t \leq p-1$ tal que $g^t \equiv a \pmod{p}$. Agora, aplique o teorema de Bézout para garantir a existência de naturais u e v tais que $nu = t + (p-1)v$, de sorte que $(g^u)^n \equiv a \pmod{p}$.

7. Considere, inicialmente, o caso em que a é ímpar. A condição do enunciado garante a existência de naturais b e t e primos ímpares distintos $q_1, \ldots, q_t$ para os quais $a = b^2 q_1 \ldots q_t$; portanto, pela proposição 7.23 de [14], basta garantirmos a existência de infinitos primos p para os quais $\left(\frac{q_1}{p}\right) \ldots \left(\frac{q_t}{p}\right) = -1$. Pela lei da reciprocidade quadrática, tal relação equivale a
$$\prod_{j=1}^{t} \left(\frac{p}{q_j}\right) = (-1)^{1+\left(\frac{p-1}{2}\right)\left(\frac{s-t}{2}\right)},$$
onde $s = \sum_{j=1}^{t} q_j$. Aplique, agora, o teorema dos primos de Dirichlet, escolhendo $p = 4kq_1 \ldots q_t + 1$.

8. Faça $\Delta = a^2 - 4b$. Multiplicando ambos os membros da equação dada por 4 e completando quadrados, mostre que as hipóteses do problema garantem que a congruência $x^2 \equiv \Delta \pmod{n}$ tem solução, para todo $n \in \mathbb{N}$. Se Δ não for quadrado perfeito, escreva $\Delta = \alpha\beta^2$, com $\alpha, \beta \in \mathbb{Z}$ e $|\alpha| > 1$. Use, então, o resultado do problema anterior para chegar a uma contradição.

Seção 8.3

1. Prove que a expansão decimal de α não é periódica.

2. Supondo que tais números fossem racionais, deduza que π e e seriam algébricos, exibindo polinômios com coeficientes racionais que teriam tais números como raízes.

3. Se $\sqrt[n]{\alpha}$ fosse algébrico, então várias aplicações do teorema 8.12 garantiriam que o mesmo sucederia com $\left(\sqrt[n]{\alpha}\right) = \alpha$. Se α^n fosse algébrico, e $f \in \mathbb{Q}[X] \setminus \{0\}$ fosse tal que $f(\alpha) = 0$, construa $g \in \mathbb{Q}[X] \setminus \{0\}$ tal que $g(\alpha) = 0$.

Seção 9.1

1. Use a relação (6.3) de [11] para estabelecer a recorrência satisfeita pelas sequências $(x_n)_{n\geq 1}$ e $(y_n)_{n\geq 1}$. Em seguida, adapte a solução do exemplo 9.4 a esse caso.

2. Se $f(X) = X^3 - 3X^2 + 1$, comece mostrando que f tem raízes reais $a > b > c$, tais que $-\frac{6}{10} < c < -\frac{5}{10}$, $\frac{6}{10} < b < \frac{7}{10}$ e $0 < b^n + c^n < 1$, para todo inteiro $n \geq 2$. Se $a_n = a^n + b^n + c^n$ para $n \geq 1$, mostre que $a_1, a_2, a_3 \in \mathbb{Z}$ e $a_{k+3} = 3a_{k+2} - a_k$, para $k \geq 1$; em seguida conclua, a partir do que fizemos acima, que $\lfloor a^n \rfloor = a_n - 1$. Por fim, use a recorrência linear satisfeita pela sequência $(a_n)_{n\geq 1}$ para mostrar que $a_{k+17} \equiv a_k \pmod{17}$; alternativamente, apele para o problema 9, página 178.

Seção 9.2

1. Para a segunda parte, suponha que $|z| > R$ e faça $\epsilon = |z| - R$. Use a condição de convergência para garantir a existência de $n \in \mathbb{N}$ tal que $|z_n - z| < \epsilon$ e deduza, daí, que $|z_n| > R$, o que é uma contradição.

2. Use o resultado do problema anterior.

3. Adapte os argumentos delineados na prova da proposição 9.15.

4. Aplique o resultado dos itens (a) e (b) do problema anterior à sequência das somas parciais de $\sum_{k\geq 1}(az_k + bw_k)$.

6. Comece observando que, se $(z_n)_{n\geq 1}$ é uma sequência em X tal que $z_n \to z$, com $z \in X$, então, pela desigualdade triangular,

$$||f(z_n)| - |f(z)|| \leq |f(z_n) - f(z)|.$$

7. Veja inicialmente que, se $(z_n)_{n\geq 1}$ é uma sequência em X, tal que $z_n \to z$, então $|z_n - z| < B$ para todo índice n suficientemente grande; daí, $|f(z_n) - f(z)| \leq A|z_n - z|$, também para todo índice n suficientemente grande. Agora, mostre que a convergência de $(z_n)_{n\geq 1}$ para z acarreta a convergência de $(f(z_n))_{n\geq 1}$ para $f(z)$.

8. O caso $m = 1$ é o conteúdo do exemplo 9.12. Para $m = 2$ e $|z| < \frac{1}{|a|}$, segue, daí, que

$$\frac{1}{(1-az)^2} = \left(\sum_{k\geq 0} a^k z^k\right)\left(\sum_{l\geq 0} a^l z^l\right) = \sum_{k,l\geq 0} a^{k+l} z^{k+l}$$
$$= \sum_{n\geq 0}(n+1)a^n z^n.$$

Por indução, se

$$\frac{1}{(1-az)^{m-1}} = \sum_{n\geq 0}\binom{n+m-2}{m-2}a^n z^n,$$

então

$$\begin{aligned}\frac{1}{(1-az)^m} &= \frac{1}{1-az}\cdot\frac{1}{(1-az)^{m-1}}\\ &= \sum_{k\geq 0} a^k z^k \cdot \sum_{l\geq 0}\binom{l+m-2}{m-2}a^l z^l\\ &= \sum_{k,l\geq 0}\binom{l+m-2}{m-2}a^{k+l}z^{k+l}\\ &= \sum_{n\geq 0}\binom{n+m-1}{m-1}a^n z^n,\end{aligned}$$

onde utilizamos o teorema das colunas do triângulo de Pascal na última igualdade acima.

Seção 9.3

2. Nas notações do enunciado da proposição 4.17, ponha $f(X) = \prod_{j=1}^{n}(1+z_jX) = \sum_{j=0}^{n} s_j X^j$; em seguida, calcule f' de duas maneiras distintas, e.g., diretamente e com o auxílio da fórmula para $\frac{f'(z)}{f(z)}$, dada no problema 3, página 83. Por fim, compare, nos casos $k < n$ e $k \geq n$, o coeficiente de X^{k-1} em ambas as expressões para f'. Você precisará utilizar o resultado do exemplo 9.12.

Referências Bibliográficas

[1] AIGNER, M. e ZIEGLER, G. (2010) *Proofs from THE BOOK.* Springer-Verlag.

[2] ANDREWS, G. (1994). *Number Theory.* Dover.

[3] AKOPYAN, A. V. e ZASLAVSKY A. A. (2007). *Geometry of Conics.* American Mathematical Society.

[4] APOSTOL, T. (1967). *Calculus, Vol. 1.* John Wiley & Sons.

[5] APOSTOL, T. (1967). *Calculus, Vol. 2.* John Wiley & Sons.

[6] APOSTOL, T. (1976). *Introduction to Analytic Number Theory.* Springer-Verlag.

[7] DE BARROS, A. A. e ANDRADE, P. F. DE A. (2009). *Introdução à Geometria Projetiva.* Sociedade Brasileira de Matemática.

[8] BARBOSA, J. L. M. (2004). *Geometria Euclidiana Plana.* Sociedade Brasileira de Matemática.

[9] BARBOSA, J. L. M. (1995). *Geometria Hiperbólica.* Instituto Nacional de Matemática Pura e Aplicada.

[10] CAMINHA, A. (2013). *Tópicos de Matemática Elementar, Volume I: Números Reais*, Segunda edição. Sociedade Brasileira de Matemática.

[11] CAMINHA, A. (2013). *Tópicos de Matemática Elementar, Volume II: Geometria Euclidiana Plana*, Segunda edição. Sociedade Brasileira de Matemática.

[12] CAMINHA, A. (2013). *Tópicos de Matemática Elementar, Volume III: Introdução à Análise*, Segunda edição. Sociedade Brasileira de Matemática.

[13] CAMINHA, A. (2016). *Tópicos de Matemática Elementar, Volume IV: Combinatória*, Segunda edição. Sociedade Brasileira de Matemática.

[14] CAMINHA, A. (2013). *Tópicos de Matemática Elementar, Volume V: Teoria dos Números*, Segunda edição. Sociedade Brasileira de Matemática.

[15] CARVALHO, P. C. P. (2002). *Introdução À Geometria Espacial.* Sociedade Brasileira de Matemática.

[16] CHERMAN, A. (2004). *Sobre os Ombros de Gigantes.* Jorge Zahar.

[17] COHEN, L. W. e EHRLICH, G. (1963). *The structure of the real number system.* D. Van Nostrand.

[18] DE MORAIS FILHO, D. C. (2012). *Um Convite à Matemática.* Sociedade Brasileira de Matemática.

[19] COURANT, R. e ROBBINS, H. (1966). *What is Mathematics?.* Oxford University Press.

[20] COXETER, H. S. M. e GREITZER, S. L. (1967). *Geometry Revisited.* The Mathematical Association of America.

[21] DIESTEL, R. (2000). *Graph Theory.* Springer-Verlag.

[22] DILWORTH, R. (1950). *A decomposition theorem for partially ordered sets*, Ann. Math. **51**, 161-166 .

[23] ERDÖS, P. e SZEKERES, G. (1935). *A combinatorial problem in geometry*, Comp. Math. **2**, 463-470.

[24] FEITOSA, S. B. (2006) *O teorema de Turán*, Sigma **3**, 2-4.

[25] DE FIGUEIREDO, D. G. (1996). *Análise I.* LTC.

[26] DE FIGUEIREDO, D. G. (2002). *Números Irracionais e Transcendentes.* Sociedade Brasileira de Matemática.

[27] GARCIA, A. e LEQUAIN, Y. (2002). *Elementos de Álgebra.* Instituto Nacional de Matemática Pura e Aplicada.

[28] GONÇALVES, A. (1999). *Introdução à Álgebra.* Instituto Nacional de Matemática Pura e Aplicada.

[29] HEATH, T. L. (1956). *The Thirteen Books of Euclid's Elements.* Dover.

[30] HILBERT, D. e COHN-VOSSEN, S. (1999). *Geometry and Imagination.* American Mathematical Society.

[31] HOFFMAN, K. e KUNZE, R. (1971). *Linear Algebra.* Prentice-Hall.

[32] HONSBERGER, R. (1985). *Mathematical Gems III.* The Mathematical Association of America.

[33] HONSBERGER, R. (1995). *Episodes in Nineteenth and Twentieth Century Euclidean Geometry.* The Mathematical Association of America.

[34] IEZZI, G. e POMPEO, J. N. (1991). *Os Fundamentos da Matemática Elementar, Vol. 9.* Atual Editora.

[35] JOHNSON, R. (2007). *Advanced Euclidean Geometry.* Dover.

[36] KLARNER, D. A. e GÖBEL, F. (1969). *Packing boxes with congruent figures.* Indag. Math. **31**, 465-472.

[37] LANDAU, E. (2002). *Teoria Elementar dos Números.* Ciência Moderna.

[38] LIMA, E. L. (1997). *Medida e Forma em Geometria.* Sociedade Brasileira de Matemática.

[39] LIMA, E. L. (2004). *Curso de Análise, Vol.* 1. Instituto Nacional de Matemática Pura e Aplicada.

[40] LIMA, E. L. (2009). *Curso de Análise, Vol.* 2. Instituto Nacional de Matemática Pura e Aplicada.

[41] LIMA, H. N. (2011). *Limites e Funções Aritméticas.* Preprint.

[42] LOZANSKY, E. e ROUSSEAU, C. (1996). *Winning Solutions.* Springer-Verlag.

[43] MITRINOVIC, D. (1964). *Elementary Inequalities.* Noordhoff.

[44] MOREIRA, C. G. e KOHAYAKAWA, Y. (2001). *Tópicos em Combinatória Contemporânea.* Instituto Nacional de Matemática Pura e Aplicada.

[45] NUSSENZVEIG, H. M. (2002). *Curso de Física Básica, Vol. 1.* Edgard Blucher.

[46] ROBERTS, J. (1978). *Elementary number theory: a problem oriented approach.* MIT Press.

[47] RUDIN, W. (1976). *Principles of Mathematical Analysis.* McGraw-Hill, Inc.

[48] SCHEINERMAN, E. (2010). *Matemática Discreta, uma Introdução.* Cengage Learning.

[49] SINGH, S. (1998). *O Último Teorema de Fermat.* Record.

[50] SOARES, M. (2014). *Cálculo em uma Variável Complexa.* IMPA.

[51] STEIN, E. e SHAKARCHI, R. (2003). *Fourier Analysis. An Introduction.* Princeton University Press.

[52] TENT, M. B. W. (2006). *Prince of Mathematics: Carl Friedrich Gauss.* A. K. Peters Ltd.

[53] TURÁN, P. (1941). *An extremal problem in graph theory.* Mat. Fiz. Lapok **41**, 435-452.

[54] VAINSENCHER, I. (1996). *Introdução às Curvas Algébricas Planas.* Instituto Nacional de Matemática Pura e Aplicada.

[55] VAN LINT, J. H. e WILSON, R. M. (2001). *Combinatorics.* Cambridge University Press.

[56] WILF, H. (1994). *Generatingfunctionology.* Academic Press.

[57] YAGLOM, I. M. (1962). *Geometric Transformations I.* The Mathematical Association of America.

CAPÍTULO A

Glossário

AIME: American Invitational Mathematics Examination.

APMO: Asian-Pacific Mathematical Olympiad.

Áustria-Polônia: Olimpíada de Matemática Austro-Polonesa.

BMO: Balkan Mathematical Olympiad.

Baltic Way: Baltic Way Mathematical Contest.

Crux: Crux Mathematicorum, periódico de problemas da Sociedade Canadense de Matemática.

IMO: International Mathematical Olympiad.

Israel-Hungria: Competição Binacional Israel-Hungria.

Miklós-Schweitzer: The Miklós-Schweitzer Mathematics Competition (Hungria).

NMC: Nordic Mathematical Contest.

OBM: Olimpíada Brasileira de Matemática.

OCM: Olimpíada Cearense de Matemática.

OBMU: Olimpíada Brasileira de Matemática para Universitários.

OCS: Olimpíada de Matemática do Cone Sul.

OIM: Olimpíada Ibero-americana de Matemática.

OIMU: Olimpíada Ibero-americana de Matemática Universitária.

ORM: Olimpíada Rioplatense de Matemática.

Putnam: The William Lowell Mathematics Competition (Estados Unidos).

Torneio das Cidades: The Tournament of the Towns, olimpíada intermunicipal mundial de Matemática.

Índice Remissivo

(*continuação dos títulos publicados*)

- *Treze Viagens pelo Mundo da Matemática* - C. Correia de Sa e J. Rocha (editores)
- *Como Resolver Problemas Matemáticos* - T. Tao
- *Geometria em Sala de Aula* - A. C. P. Hellmeister (Comitê Editorial da RPM)
- *Números Primos, amigos que causam problemas* - P. Ribenboim
- *Manual de Redação Matemática* - D.C de Morais Filho

COLEÇÃO PROFMAT

- *Introdução à Álgebra Linear* - A. Hefez e C.S. Fernandez
- *Tópicos de Teoria dos Números* - C. G. Moreira , F. E Brochero e N. C. Saldanha
- *Polinômios e Equações Algébricas* - A. Hefez e M.L. Villela
- *Tópicos de Historia de Matemática* - T. Roque e J. Bosco Pitombeira
- *Recursos Computacionais no Ensino de Matemática* - V. Giraldo, P. Caetano e F. Mattos
- *Temas e Problemas Elementares* - E. L. Lima, P. C. Pinto Carvalho, E. Wagner e A. C. Morgado
- *Números e Funções Reais* - E. L. Lima
- *Aritmética* - Abramo Hefez
- *Geometria* - A. Caminha
- *Avaliação Educacional* - M. Rabelo
- *Geometria Analítica* - J. Delgado, K. Frensel e L. Crissaff
- *Matemática Discreta* - A. Morgado e P.C.P. Carvalho
- *Matemática e Atualidade - Volume 1* - C. Rousseau e Y. Saint-Aubin

COLEÇÃO INICIAÇÃO CIENTÍFICA

- *Números Irracionais e Transcendentes* - D. G. de Figueiredo
- *Números Racionais e Irracionais* - I. Niven
- *Tópicos Especiais em Álgebra* - J. F. S. Andrade

COLEÇÃO TEXTOS UNIVERSITÁRIOS

- *Introdução à Computação Algébrica com o Maple* - L. N. de Andrade
- *Elementos de Aritmética* - A. Hefez
- *Métodos Matemáticos para a Engenharia* - E. C. de Oliveira e M. Tygel
- *Geometria Diferencial de Curvas e Superfícies* - M. P. do Carmo
- *Matemática Discreta* - L. Lovász, J. Pelikán e K. Vesztergombi
- *Álgebra Linear: Um segundo Curso* - H. P. Bueno

(*continuação dos títulos publicados*)

- *Introdução às Funções de uma Variável Complexa* - C. S. Fernandez e N. C. Bernardes Jr.
- *Elementos de Topologia Geral* - E. L. Lima
- *A Construção dos Números* - J. Ferreira
- *Introdução à Geometria Projetiva* - A. Barros e P. Andrade
- *Análise Vetorial Clássica* - F. Acker
- *Funções, Limites e Continuidade* - P. Ribenboim
- *Fundamentos de Análise Funcional* - D. Pellegrino, E. Teixeira e G. Botelho
- *Teoria dos Números Transcendentes* - D. Marques
- *Introdução à Geometria Hiperbólica - O modelo de Poincaré* - P. Andrade
- *Álgebra Linear: Teoria e Aplicações* - T. P. de Araújo

COLEÇÃO MATEMÁTICA APLICADA

- *Introdução à Inferência Estatística* - H. Bolfarine e M. Sandoval
- *Discretização de Equações Diferenciais Parciais* - J. Cuminato e M. Meneguette

COLEÇÃO OLIMPÍADAS DE MATEMÁTICA

- *Olimpíadas Brasileiras de Matemática, 1ª a 8ª* - E. Mega, R. Watanabe
- *Olimpíadas Brasileiras de Matemática, 9ª a 16ª* - C. Moreira, E. Motta, E. Tengan, L. Amâncio, N. C. Saldanha e P. Rodrigues
- *21 Aulas de Matemática Olímpica* - C. Y. Shine
- *Iniciação à Matemática: Um Curso com Problemas e Soluções* - K. I. M. Oliveira e A. J. C. Fernández
- *Olimpíadas Cearenses de Matemática 1981-2005 Nível Fundamental* - E. Carneiro, O. Campos e M.Paiva
- *Olimpíadas Cearenses de Matemática 1981-2005 Nível Médio* - E. Carneiro, O. Campos e M.Paiva
- *Olimpíadas Brasileiras de Matemática - 17ª a 24ª* - C. G. T. de A. Moreira, C. Y. Shine, E. L. R. Motta, E. Tengan e N. C. Saldanha

COLEÇÃO FRONTEIRAS DA MATEMÁTICA

- *Fundamentos da Teoria Ergódica* - M.Viana e K. Oliveira
- *Tópicos de Geometria Diferencial* - A. C. Muniz Neto
- *Formas Diferenciais e Aplicações* - M. Perdigão do Carmo